23932
PATENT TRADEMARK OFFICE

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

TITLE:

AN IMPROVED VIRTUAL PRIVATE SWITCHED TELECOMMUNICATIONS NETWORK

INVENTORS:

GREG SCHMID

KEITH S. PICKENS

KIRK SMITH

CRAIG HEILMANN

CERTIFICATE OF MAILING 37 C.F.R. § 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail, Express Mail No. EV 002012749 US, addressed to: Mail Stop Patent Application/FEE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450; on July 23, 2003.

Venisa J. Dark
Name of Person Filing or Mailing Document

Venisa J. Dark
Signature of Person Mailing or Filing Document

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit under Title 35 United States Code 119(e) of U.S. Provisional Application No. 60/307,209, filed July 23, 2002, entitled "A System and Method for Encapsulation, Compression and Encryption of PCM Data" and claims benefit from U.S. Patent Application No. 09/907,089, filed July 17, 2001, entitled "Telephony Security System" and claims benefit from U.S. Patent Application No. 09/709,592, filed November 10, 2000, entitled "A System and Method for Encapsulation, Compression and Encryption of PCM Data", all assigned to the assignee of the present invention and incorporated herein by reference.

TECHNICAL FIELD

[0002] The invention relates generally to telecommunications access control systems and more particularly, to a system and method whereby a virtual private switched telecommunications network is autonomously constructed between at least two in-line devices.

BACKGROUND OF THE INVENTION

[0003] In the past several years, as interception and penetration technologies have multiplied, information assets have become increasingly vulnerable to interception while in transit across untrusted networks between the intended parties. The increasing prevalence of digital communications systems has led to the widespread use of digital encryption systems

by governments and enterprises concerned with communications security. These systems have taken several forms, from data Virtual Private Networks (VPN), to secure voice/data terminals.

[0004] Enterprises are communicating using voice, fax, data modem, and video across the untrusted Public Switched Telephone Network (PSTN). Unfortunately, whereas a data VPN uses automated encryption and tunneling processes to protect information traveling over the Internet, a data VPN is not designed to protect voice, fax, modem, and video calls over the untrusted PSTN. This deficiency leaves solutions for creating safe tunnels through the PSTN to be primarily manual, requiring user participation at both ends to make a call secure (e.g., with the use of secure voice/data terminals, such as Secure Telephone Units (STU-IIIs), Secure Telephone Equipment (STE), and hand-held telephony encryption devices).

[0005] Additionally, secure voice/data terminals are point-to-point devices securing only one end-user station per device; so secure voice/data terminals cannot protect the vast majority of calls occurring between users who do not have access to the equipment. And although there may be policies that specifically prohibit it, sensitive material can be inadvertently discussed on non-secure phones and thereby distributed across the untrusted PSTN.

[0006] Secure voice/data terminals cannot implement an enterprise-wide, multi-tiered policy-based enforcement of a corporate security policy, establishing a basic security

structure across an enterprise, dictated from the top of the tier downward. Neither can secure voice/data terminals implement an enterprise-wide, multi-tiered policy-based enforcement of selective event logging and consolidated reporting (i.e., multi-tiered policy-based security event notification) to be relayed up the tier.

[0007] Lastly, secure voice/data terminals cannot provide call event logs detailing information about secure calls. Therefore, a consolidated detailed or summary report of a plurality of call event logs can not be produced for use by security personnel and management in assessing the organization's security posture.

[0008] Clearly, there is a need for a system and method to provide secure access across the untrusted PSTN through telephony resources that can be initiated by a security policy defining actions to be taken based upon zero or more attributes of the call, providing secured communications operating as a data call at 64Kbps, with automatic adjustment to circuits operating at 56Kbps or slower, and providing multi-tiered policy-based enforcement capabilities, multi-tiered policy-based security event notification capabilities, and visibility into security events.

[0009] As used herein, the following terms carry the connotations described below:

- Data VPN is understood to refer to a shared or public packet data network wherein privacy and security issues are mitigated through the use of a combination of authentication, encryption, and tunneling.

- Tunneling is understood to refer to provision of a secure, temporary path over an Internet Protocol (IP)-based network by encapsulating encrypted data inside an IP packet for secure transmission across an inherently insecure IP network, such as the Internet.
- Secure is understood to refer to the use of encryption to provide telecommunications privacy and security between two devices across an untrusted network (as discussed herein and specifically with reference to Figures 1,11A-11D, 12, 13A-13E, and 16); or the result thereof.
- Data call is understood to refer to a call using a bearer service that is circuit mode, with either 64Kbps information transfer rate or 64Kbps information transfer rate adapted to 56 Kbps, that uses unrestricted or restricted digital information transfer capability.
- Voice call is understood to refer to a call using a bearer service that is circuit mode, with speech or 3.1 kHz audio information transfer capability and user information layer 1 protocol G.711 mu-law or A-law.

SUMMARY OF THE INVENTION

[0010] A system and method to provide secure access across the untrusted PSTN is described, hereafter to be referred to as a Virtual Private Switched Telecommunications Network (VPSTN). The VPSTN creates a virtual private network, i.e., "secures"

telecommunications, across a public untrusted network between two in-line devices by encrypting calls in accordance with a security policy. The security policy defines actions to be taken based upon zero or more attributes of the call.

[0011] If the local security policy dictates that a secure call is to be initiated by the local in-line device, and the attempt to conduct the call in secure mode is acknowledged by the remote in-line device (in accordance with the remote security policy), the VPSTN will initiate encryption on the bearer channel using select administrator-allowed secure modes.

[0012] The initiating local in-line device intercepts and modifies the call setup message from the PBX, changing it from a request for bearer capability to support a voice call to a request for bearer capability to support a data call at 64Kbps (data at 64Kbps). Because the call is sent across the PSTN as a data call, network echo suppressors, digital pads, and other digital impairments are not present, and therefore do not need to be disabled or taken into account when transmitting.

[0013] If the data call fails due to network issues (such as a trunk is not capable of supporting unrestricted data at 64Kbps), the VPSTN autonomously falls back through each of its allowed data call secure modes (based on administrator configuration and in accordance with the security policy) until the call is connected.

[0014] If all allowed data call secure modes are exhausted, the VPSTN autonomously falls back to allowed voice call secure modes (based on administrator configuration and in accordance with the security policy), which utilizes ADPCM

compression, echo canceller disable tone, and processes similar to Digital Impairment Learning (DIL). Voice call secure modes may include voice at 56Kbps using no compression, and voice at 48Kbps, voice at 40Kbps, voice at 32Kbps, and voice at 24Kbps using 5-bit, 4-bit, 3-bit, and 2-bit ADPCM respectively. Using the least amount of compression will achieve the highest quality signal. Alternatively, in accordance with the security policy, the VPSTN can transmit the call using clear voice (without encryption).

[0015] Some primary advantages of the disclosed system and method are: (1) secure transport of voice, fax, modem, and VTC calls across the PSTN; (2) automatic discovery of called and calling party's capability to support secured communications; (3) automatic discovery of a digital signal level 0 (DS-0) channel's line impairments and capability to support secured communications; (4) automatic detection that a received DS-0 TDM serial stream is VPSTN-compatible; (5) provision of secured communications with automatic disabling of secured communications responsive to a PBX's request for a data call; (6) automatic compression and decompression of the payload portion of the call when providing secured communications on channels operating at 56Kbps or slower; (7) operator-transparency, i.e., neither call party is required to take any specific actions in order to initiate or conduct secure communications; (8) provision of secured communication for multiple end-user stations per device (i.e., secured communication is selectively provided for all calls routed on trunks in which the in-line device is deployed); (9) implementation and enforcement of a security policy designating all inbound and outbound calls are automatically

conducted in secure mode whenever possible, based on zero or more attributes of the call; (10) implementation and enforcement of a security policy designating that select calls are conducted in secure mode based on one or more designated attributes of the call; (11) implementation and enforcement of a security policy designating that select calls are allowed or denied and other designated actions are performed responsive to the success or failure to conduct a call in secure mode; (12) creation of a VoIP-compatible packet from the data contained in the TDM serial stream; (13) encapsulation of a VoIP-compatible packet within the secured media payload to support transport over the synchronous time division multiplexed PSTN network; (14) automatic synchronization of packets from one or more diverse remote VPSTN-compatible systems; (15) implementation and enforcement of a security policy designating that select calls are allowed or denied and other designated actions are performed based on one or more designated attributes of the call; (16) implementation and enforcement of a basic security structure and policy across an enterprise, dictated from the top of the tier downward; and (17) implementation and enforcement of an enterprise-wide policy of selective event logging and consolidated reporting to be relayed up the tier.

[0016] Some secondary advantages of the disclosed system and method are: (1) policy-based selection of static secret session keys, key exchange mechanisms, and encryption algorithms based on one or more designated attributes of the call; (2) secured communications transparent to the transcoding within the PSTN; (3) automatic compensation

when transcoding occurs within the PSTN during secure transport; (4) selectively provided audible feedback to the calling or called parties indicating the secure state of the call; (5) a message channel transported separate from and concurrent with the secured payload portion of the call; (6) the message channel stays active throughout the duration of the call; (7) secure communications can be initiated or discontinued while the call is in progress; (8) automatic generation and exchange of new keys for each session; (9) automatic disabling of secured communications responsive to detection of designated call-type.

[0017] Therefore, in accordance with the previous summary, objects, features, and advantages of the present invention will become apparent to one skilled in the art from the subsequent description and the appended claims taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] A better understanding of the system and method for autonomously constructing a virtual private switched telecommunications network between at least two in-line devices may be had by reference to the drawing figures wherein:

Figure 1 is a schematic block diagram illustrating an exemplary virtual private switched telecommunications network of the present invention;

Figure 2 is a schematic block diagram illustrating a portion of the exemplary virtual private switched telecommunications network of Figure 1;

Figure 3 is a functional schematic block diagram illustrating a simplified example security policy and corresponding actions and features of the virtual private switched telecommunications network of Figure 1;

Figure 4 is a functional schematic block diagram illustrating simplified example security policy elements and interactions of the virtual private switched telecommunications network of Figure 1;

Figures 5A and 5B are a process flow diagram illustrating installation, configuration, and operational processes of the virtual private switched telecommunications network of Figure 1;

Figures 6A and 6B are a table illustrating a portion of an example user group listing for use by the virtual private switched telecommunications network of Figure 1;

Figures 7A and 7B are a table illustrating a portion of an example security rule base for use by the virtual private switched telecommunications network of Figure 1;

Figures 8A, 8B, and 8C are a table illustrating a portion of an example result response policy for use by the virtual private switched telecommunications network of Figure 1;

Figure 8D is a table illustrating a "Secure All Possible Calls" alternate security rule base for use by the virtual private switched telecommunications network of Figure 1;

Figure 8E is a table illustrating a "Secure All Possible Calls" alternate result response policy for use by the virtual private switched telecommunications network of Figure 1;

Figures 9A and 9B are a process flow diagram illustrating detection and analysis of call activity and implementation of the security rule base by the virtual private switched telecommunications network of Figure 1;

Figures 10A and 10B are a process flow diagram illustrating evaluation of the results of the secure call attempt and implementation of the result response policy by the virtual private switched telecommunications network of Figure 1;

Figure 11A is a schematic block diagram illustrating subrate channels and bit assignments in a VPSTN 100 DS-0 channel sample for data call secure mode at 64Kbps;

Figure 11B is a schematic block diagram illustrating subrate channels and bit assignments in a VPSTN 100 DS-0 channel sample for data call secure mode at 56Kbps and voice call secure mode at 56Kbps;

Figure 11C is a schematic block diagram illustrating subrate channels and bit assignments in a VPSTN 100 DS-0 channel sample for voice call secure mode at 48Kbps;

Figure 11D is a schematic block diagram illustrating an example structure of the VPSTN 100 DS-0 packet made up of the channel samples of Figures 11A, 11B, or 11C;

Figure 12 is a process flow diagram illustrating the process whereby the virtual private switched telecommunications network of Figure 1 conducts a call in secure mode;

Figures 13A and 13B are a process flow diagram illustrating setup and conduction of a call in secure mode by the virtual private switched telecommunications network of Figure 1, wherein the DS-1 circuit includes ISDN PRI access trunks;

Figures 13C, 13D and 13E are a process flow diagram illustrating setup and conduction of a call in secure mode by the virtual private switched telecommunications network of Figure 1, wherein the DS-I circuit includes T1 access trunks;

Figure 14 is a schematic block diagram illustrating distributed deployment of the virtual private switched telecommunications network of Figure 1;

Figures 15A and 15B are a schematic block diagram illustrating deployment of the virtual private switched telecommunications network of Figure 1 for multi-tiered policy-based enforcement of a security policy across a large, globally distributed enterprise;

Figures 15C, 15D, and 15E are a table illustrating a portion of an example security rule base for use in implementing multi-tiered policy-based enforcement of the security policy;

Figure 15F is a process flow diagram illustrating implementation of the multi-tiered policy-enforcement of the security policy;

Figure 15G is a process flow diagram illustrating implementation of filtering on "Track" tasks in a multi-tiered policy-enforced environment; and

Figure 16 is a schematic block diagram illustrating use of computer telephony integration to complement the portion of the virtual private switched telecommunications network of Figure 2.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0019] The present invention can be described with several examples given below. It is understood, however, that the examples below are not necessarily limitations to the present invention, but are used to describe typical embodiments of operation.

5

Virtual Private Switched Telecommunications Network

[0020] Figure 1 is a schematic block diagram of an exemplary Virtual Private Switched Telecommunications Network (VPSTN) 100 of the present invention, similar to the telecommunications firewall implemented as shown and described in U.S. Patent 10 Application Serial No. 09/210,347, now U.S. Patent No. US 6,249,575 B1. The VPSTN 100 can be combined with the telecommunications firewall to act as an integrated VPSTN 100 and a firewall simultaneously, or to result in a mixture of capabilities of each device.

[0021] The VPSTN 100 includes at least two in-line devices such as Telephony Appliances (TA) 102 and 104, management servers 106 and 108, and clients 110 and 112, all 15 interconnected by a Transmission Control Protocol/Internet Protocol (TCP/IP)-based Local Area Network (LAN), Wide Area Network (WAN), or the Internet (any of which are identified herein with numeral 113), for interaction as described below. The inventive functions described herein as being performed by the TA 102, management server 106, and client 110 are similarly performed by the TA 104, management server 108, and client 112, as

well as subsequent embodiments of telephony appliances, management servers and clients discussed herein.

[0022] The VPSTN 100 provides secure communication between two geographically separate, even globally distributed, locations. The TA 102 and 104 are installed in-line on a DS-1 circuit. The capacity (i.e., quantity and speed of channels) on a DS-1 circuit varies relative to global location. For instance, a Trunk level 1 (T1) or J1 line (or trunk), used in North America and Japan respectively, operates at 1,544,000 bits per second (bps) and carries 24 time-division-multiplexed (TDM) Digital Signal level 0 (DS-0) channels. Additionally, in North America, an Integrated Services Digital Network Primary Rate Interface (ISDN PRI) trunk may carry either 23 TDM DS-0 channels and one signaling channel, or 24 TDM DS-0 channels. In Europe, an E1 trunk operates at 2,048,000 bps and carries 30 TDM DS-0 channels in addition to 2 signaling channels. A DS-0 channel operates at 64,000 bps, which is the worldwide standard speed for digitizing one voice conversation using Pulse Code Modulation (PCM) and sampling the voice 8,000 times per second and encoding the result in an 8-bit code (8 x 8000 = 64,000 bps). An additional variation relative to global location is the difference in the form of PCM encoding. Typically, mu-law is the standard used in North American and Japanese telephone networks, and A-law is used in European and most other national public switched telephone networks. Transcoding, or modifying the data stream from mu-law to A-law so that it can be carried via a different network, may cause the PCM value to change. Regardless of whether the T1, J1, ISDN PRI,

E1, etc., trunk carrying the DS-1 circuit between the VPSTN 100 and the PSTN is the same on both sides of the PSTN (i.e., T1 trunk to PSTN to T1 trunk, as may occur with calls conducted within North America), or is some combination of trunk types (i.e., T1 trunk to PSTN to E1 trunk, as would occur with an international call between North America and Europe), all operations are transparent to the individuals placing and receiving the call (i.e., neither call party is required to take any specific actions in order to initiate or conduct a secure call).

[0023] The TA 102 is installed in-series on a DS-1 circuit 103, within the enterprise (as shown in Figure 2), in locations such as between a Public Branch eXchange (PBX) 114 and a Public Switched Telephone Network (PSTN) 116. The TA 104 is similarly installed in-series on the DS-1 circuit 105, in locations such as between the PSTN 116 and a PBX 118. The TA 102 has two input and two output ports; specifically, a PBX-in port 120, a PSTN-out port 122, a PSTN-in port 124, and a PBX-out port 126. Similarly, the TA 104 has two input and two output ports; specifically, a PSTN-in port 128, a PBX-out port 130, a PBX-in port 132, and a PSTN-out port 134.

[0024] Figure 1 shows the full-duplex nature of the VPSTN 100 with the transmit channel and the receive channel fully encrypted and decrypted, respectively. The TA 102 and 104 each control operational aspects of the transmit channels they produce. Specifically, the TA 102 controls the transmit channel that makes up links from the PSTN-out port 122 to the PSTN 116 and from the PSTN 116 to the PSTN-in port 128, represented by numerals 156

and 158, respectively. The TA 104 controls the transmit channel that makes up links from the PSTN-out port 134 to the PSTN 116 and from the PSTN 116 to the PSTN-in port 124, represented by numerals 160 and 162, respectively. Therefore, the TA 102 controls the TA 104 receive channel (the links 156 and 158) and the TA 104 controls the TA 102 receive channel (links 160 and 162).

[0025] The client 110 and 112 is a point of user-interface for the system administrator configuring a security policy, displaying and viewing real-time alerts, viewing real-time event logs, printing event logs and consolidated reports, and other operational features of the VPSTN 100.

[0026] As discussed in more detail with reference to Figures 3, 4, 7A-7B, and 8A-8C, a security policy is a sequential listing of rules that define whether certain calls to or from an end-user station 136 or 138 will be allowed, denied (terminated), conducted in secure mode, reported, logged, etc. The security policy also defines whether other additional actions such as sending a tone or message to call parties to, for example, indicate the ability or inability to conduct the call in secure mode, and sending notifications such as electronic mail notification, pager alerting, console messaging, or a Simple Network Management Protocol (SNMP) trap notification are required.

[0027] The management server 106 and 108 receive the security policy from the client 110 and 112, and push a copy of the security policy to the TA 102 and 104, respectively. The management server 106 and 108 are connected to the TA 102 and 104,

respectively, for consolidation and management of reports and call logs. Historical logging and archiving of calls, pursuant to a predetermined security policy, may be accomplished on the local management server, or stored via a network-accessible log server (not shown).

[0028] The TA 102 and 104 receive the security policy, and as appropriate, monitor inbound and outbound calls, allow, deny, or otherwise manipulate calls, including conducting calls in secure mode, all pursuant to the security policy, and based on at least one call attribute e.g., call type (voice, fax, modem, VTC, etc.).

[0029] The TA 102 and 104 may combine call-progress monitoring, caller-id (CND) and/or Automatic Number Identification (ANI) decoding, digital line protocol reception, decoding, demodulation, pulse dial detection, Dual-Tone MultiFrequency (DTMF) and MultiFrequency (MF) tone detection, compression, encryption, decryption, and decompression with microprocessor control, access-control logic, and call-interrupt circuitry for implementing the desired VPSTN functions. The inventive functions performed by the TA 102 and 104, as further described below, may be implemented with commercially available components, as will be understood by those skilled in the art. While also not shown, it is understood that the TA 102 and 104 are controlled by computer programming instructions stored in memory within the TA 102 and 104, and which may also be stored in memory within other components of the VPSTN 100 connected to the TA 102 and 104.

[0030] Also in Figure 1, numerals 136 and 138 designate end-user stations, representing as examples, one or more modems 140 and 142, fax machines 144 and 146,

telephones 148 and 150, and VTC stations 149 and 151, which may send or receive calls over the VPSTN 100. The modems 140 and 142 may support a desktop or portable personal computer, for example. Individual station extensions 152 and 154 connect the end-user stations 136 and 138 to the PBX 114 and 118, respectively, or to a Central Office (CO) 208 within the PSTN 116 (as shown in Figure 2).

[0031] For clarity and simplicity of explanation, Figure 1 and subsequent figures (except when described otherwise), show a complete DS-1 circuit connected between the TA 102, the PSTN 116, and the TA 104; although typically, the DS-0 channels that make up the DS-1 circuit may be individually switched by the PSTN 116 to different locations, relevant to call destination. It is understood that a security policy can be configured such that the VPSTN 100 is selectively applied to calls, based on at least one call attribute such as the call direction (inbound, outbound); the call source number; the call destination number; call type; the date; the time; the call duration (not shown), etc., as shown in Figures 7A-7B. Additionally, in the examples provided, voice is the media transported, although the present invention also provides secure transport for media in addition to voice, including fax, modem and VTC. The examples are also based on use of the Triple Data Encryption Standard (3DES) encryption algorithm, although other encryption algorithms, including DES, Advanced Encryption Standard (AES), and International Data Encryptions Algorithm (IDEA) may be used.

[0032] Additionally, the system and method supports distributed deployment, as well as a system and method of multi-tiered policy-based enforcement of a security policy, as described later with reference to Figure 14 and Figures 15A-15G.

[0033] Figure 2 is a schematic block diagram of a portion 200 of the exemplary VPSTN 100 of Figure 1. Numerals 202 and 206 represent configurations whereby connectivity of the TA 102 may be accomplished; including any combination of one or more of either: the TA 202 (on direct lines from the CO 208); and the TA 206 (on the trunk-side of the PBX 114). The TA 202 and the TA 206, the management server 106, and client 110, are connected by the LAN, the WAN, or the Internet 113.

[0034] As represented by the TA 202 and its corresponding lines, it is understood that the TA 202 is configured to map one or more circuits through the TA 202 to their direct connection to the CO 208. For clarity and simplicity of explanation, subsequent references to TA 102 shall refer to either of the TA 202 and 206, except when specifically described otherwise.

[0035] Referring also to Figure 3, a functional schematic block diagram 300 illustrates certain operational aspects of the VPSTN 100 of Figure 1. An example (very simplified) security policy 302 is shown for controlling the flow of calls through the VPSTN 100. It is understood that the rule-set is implemented by software instructions within the TA 102 that may, for example, be programmed or modified at either the TA 102 or at the

management server 106 and client 110 (Figure 1) located nearby or at a very remote distance therefrom.

[0036] As exemplified in Figure 3, the security policy 302 dictates the type of actions associated with individual or groups of calls (e.g., allow, deny, conduct the call in secure mode, log, alert, report), pursuant to specified rules. In the present example, the security rules specify that: (1) voice, fax, modem, and VTC calls to a certain destination or from a certain source identified by a digital sequence (e.g., "*XXX**," where "*XXX* " indicates the country code for Country *X* followed by the number "*"), should be conducted in secure mode; (2) voice, fax, modem, and VTC calls to a certain inbound destination or from a certain outbound source should be conducted in secure mode; (3) voice, fax, modem, and VTC calls to a certain outbound destination or from a certain inbound source will be conducted in secure mode; (4) fax calls to a certain inbound destination at a certain time or within a certain time period will be conducted in secure mode; (5) modem calls to a certain inbound destination will be conducted in secure mode.

[0037] A call log 304 is constructed for each call, consisting of concatenated call event records designating attributes of the calls. The call logs 304 are stored in a database on the management server 106. Real-time ongoing and historical call log(s) 304 are viewed and printed from the management server 106. The call log 304 for each call is generated to an administrator-designated level of detail, ranging from very brief to verbose. While the call log 304 shown in Figure 3 is a very simplified example, the detail of the call log 304 ranges

from including all call attributes, all call events, and all actions taken on the call, to including only selected call attributes, call events, and actions taken against the call.

[0038] Configuration of the call log 304 details and the security policy 302 rule-sets may include one or more of the following call attributes and rule criteria:

- Call Key - a unique identifying key assigned to each call by the TA 102;
- Line - the identifier for the extension or direct connect line carrying the call;
- Trunk - the PBX trunk group through which the call is processed;
- Channel - the channel through which the call is processed;
- TA 102 Name - the designated alias of the TA 102 processing the call and enforcing the rule;
- TA 102 Group - the designated alias of the group (or array of TA(s) 102) to which the TA 102 processing the call belongs;
- Start Date - the start date of the call;
- Start Time - the start time of the call;
- Direction - whether the call is inbound or outbound;
- Raw Destination Digits – the digits dialed prior to call connection, including prefix digits, the base phone number and suffix digits;

- Prefix – all digits dialed before the base phone number, such as outside access number or long distance access code;
- Suffix – all digits dialed after the base phone number, such as DTMF-based PIN code used in authentication for remote access, or calling card numbers;
- Source - number, or mask (e.g., 210-402-XXXX) where the source number is the number of the party initiating the call; i.e., the extension assigned to a station for outbound calls, or the number extracted from caller-ID (or any other means) for inbound calls;
- Source Name – caller ID alias or identifier;
- Destination - number, or mask where the destination number is the number of the party receiving the call; i.e., the extension assigned to a station for inbound calls, or the number dialed (DTMF decoded or by any other means) for outbound calls;
- Connect Time - the time at which the call was answered (connected);
- Call-Type - the type of call, based either on equipment or call progress events (e.g., voice, fax, modem, VoIP, STU-III-data, STU-III-voice, STU-III-unspecified, STE, wideband, wideband video, and busy, unanswered, undetermined);
- Call Content – designated keywords detected in voice, VoIP, and modem calls;
- Actions – designated actions executed by the TA 102, pursuant to the security policy (i.e., allow or deny the call);

- Tracks – additional actions and tracking functions executed, pursuant to the security policy (e.g., TA 102 additional actions include: conduct the call in secure mode, send a tone or message, record call content, redirect the call, authenticate remote access, monitor call content for keywords, conduct the call in secure mode, transport the call using VoIP; management server 106 tracking functions include: adjust the security policy, log call events, and generate notification alerts and reports);
- Redirect – the port and name of the peripheral device the call is redirected to;
- Post-connect digits – digits dialed after the call is connected;
- Log Time - the date and time a call event record is appended to the call log 304;
- End Date - the date the call ended;
- End Time - the time of day the call ended;
- Duration - the duration of the call (in seconds).

[0039] Several reports, including a post-event report 303, a schedule-generated report 305, or an ad hoc report 307 may be initiated, or scheduled for later generation and delivery, via a graphical user interface-based report module (not shown) within the management server 106. The report module consolidates and manages designated call log 304 data for use in assessing an enterprise's telephony resource usage and/or security posture.

[0040] Reports are configuration-edited, generated, archived, displayed and printed via the management server 106. Report criteria includes: the date/time range for which call

log data will be retrieved; call log 304 fields to be used; data organization (sorting, filtering, grouping, ordering); data presentation level (in detail or high level summary); and data display format (charts, graphs, or trends).

[0041] The post-event report 303 contains predefined information concerning a specified call event and is generated responsive to the call event, and pursuant to the security policy 302.

[0042] The schedule-generated report 305 contains previously designated categories of call log data and is automatically generated, displayed, printed, and delivered at previously designated, discrete or recurring times and/or days. The schedule-generated report 305 is delivered to the designated recipient(s) by electronic mail message, to the designated file directory on a network- or web-accessible server, and/or to the designated archival file directory. It is understood that any configurable report, and any number of reports may be scheduled for generation and display, printing, or delivery at any discrete time or number of recurring time(s).

[0043] The ad hoc report 307 is manually initiated by authorized personnel. Both the schedule-generated report 305 and the ad hoc report 307 may include, for example, batch analysis of call log data for a trend or difference/comparison report 306, either in great detail or high-level summary.

[0044] The management server 106 generates several types of alerts pursuant to the security policy 302, including, for example: electronic mail notification 308, pager alerting

310, console messaging, and SNMP trap notification (not shown). Alert contents are administrator-configurable, derived from call log 304 data. While not shown, it is understood that the VPSTN 100 is able to communicate within the enterprise network with various host computers for providing the reporting and alert functions.

Security Policy

[0045] Figure 4 is a functional schematic block diagram of an exemplary security policy 302 for enforcement by the VPSTN 100 of Figure 1. In a preferred embodiment, the security policy 302 includes a security rule base 402, a result response policy 404, and a plurality of groups represented by numeral 406. Although a plurality of security rule bases, such as the security rule base 402, with a plurality of corresponding result response policies, such as the result response policy 404, can be configured for a large globally distributed enterprise, for the sake of simplicity and clarity, only one of each component is shown in this diagram.

[0046] The security rule base 402, result response policy 404, and groups 406 are used by the VPSTN 100 to control calls and respond to vulnerabilities (e.g., when the security policy 302 requires that a call be conducted in secure mode, but the attempt to conduct a secure call fails). The security rule base 402, discussed in further detail later with reference to Figures 7A-7B, is a sequential listing of rules that defines whether certain calls to an extension will be allowed or denied (hung-up), and logged, or if other actions such as

conducting the call in secure mode will be initiated, and if electronic mail notification, pager alerting, console messaging, or SNMP trap notification are required.

[0047] The result response policy 404, discussed in further detail later with reference to Figures 8A-8C, is a sequential listing of response rules (similar in construction to the security rule base 402), which defines the appropriate response to the results of defined actions, such as the ability or inability to conduct a call in secure mode. Add from late 1300s that the policy may be configured to dictate select responses based on the reason for failure to conduct the call in secure mode. The result response policy 404 defines whether the results will be logged, whether the call will be allowed or denied, whether a tone or message will be played to call parties, and whether notifications such as electronic mail notification, pager alerting, console messaging, or SNMP trap notification to designated system or security personnel, and automatic adjustments to the contents of groups 406 (and hence to the security policy 302), will be executed.

[0048] It is contemplated that the VPSTN 100 will make extensive use of groups, where objects of the same type can be collectively referred to by a meaningful alias. Groups 406, discussed in further detail later with reference to Figures 6A-6B, are used by both the security rule base 402 and the result response policy 404 to indicate and "bundle" specific extensions for convenience in applying the security policy 302. When dictated by the result response policy 404, the management server 106 adjusts the security policy 302 by moving an extension from its current group within group 406 to a different designated group within

group 406. Although not shown, the use of various types of objects and groups of objects by both the security rule base 402 and the result response policy 404 in applying the security policy 302, such as groups of designated static secret keys, key exchange mechanisms, and encryption algorithms, are contemplated.

[0049] Whether the TA 102 attempts and succeeds, or attempts and fails to establish and conduct the call in secure mode, the TA 102 references the result response policy 404 to determine the appropriate response to the success or failure. When the result response policy 404 rule is matched, the TA 102 allows or denies the call, may play a tone or message, and notifies the management server 106 that the rule has fired, pursuant to the result response policy 404. The management server 106 references the fired result response policy 404 rule to determine the appropriate response to the success or failure of the attempt. Responses may include sending notifications such as electronic mail notification, pager alerting, console messaging, or a SNMP trap notification, logging the event, and adjusting the security policy by moving the extension from its current group to a different group.

[0050] For example, assume that a daily inbound call is placed from the Chicago branch office to one of the modems in the daily receivable modem group, for the purpose of reporting the day's receipts. Since the daily receipts are confidential information, the security rule base 402 includes the following rule: "Allow inbound modem calls to extensions in the daily receivable modem group, conduct the call in secure mode, and log the call."

[0051] The result response policy 404 includes the following rule: "Allow inbound modem calls to extensions in the daily receivable group that are successfully conducted in secure mode and log the event;" and "Deny inbound modem calls to extensions in the daily receivable group that fail to be conducted in secure mode, play a tone, generate an electronic mail notification and a pager alert, and log the event. If the attempt to conduct the call in secure mode fails, the daily receivable modem extension is moved from the daily receivable modem group to the VPSTN non-secure group."

[0052] Pursuant to the security rule base 402, and as described later with reference to Figures 13A–13E, the inbound modem call to the daily receivable modem group will be conducted in secure mode. If the call can not be conducted in secure mode, pursuant to the result response policy 404, the TA 102 plays a tone and denies the call. The management server 106 generates an email and page, logs the call, and moves the extension from the daily receivable modem group to the VPSTN non-secure group, thereby denying any future modem traffic on the extension.

Installation, Configuration, and Operation

[0053] Figures 5A and 5B collectively illustrate a process flow diagram 500 of the installation, configuration and operation processes for the VPSTN 100 of Figure 1. Once installed and configured, it is understood that the VPSTN 100 is capable of operating in a continuous processing loop, including detecting call attributes and analyzing call activity,

while simultaneously performing appropriate actions (e.g., initiating and conducting calls in secure mode), pursuant to the rules in the defined security policy 302. There are, however, a number of processes that are first performed as part of the installation and configuration of the VPSTN 100 within an enterprise, or one or more of its locations.

[0054] Step 502 refers to the process of system installation and hardware configuration. The TA 102 are installed in-line, as shown by TA 202 and 206 in Figure 2. The management server 106, and client 110 are set up, whereby personal computers, meeting certain performance specifications, are acquired and configured with an operating system, booted, and made ready for operation. Software required to operate the VPSTN 100, including for example defining and maintaining the security policy 302, is installed onto the management server 106. Although not shown, it is understood that installation of control software may include writing firmware instructions for the associated switches and/or the associated control logic for the TA 102, as required. The TA 202 assigns telephone numbers to direct connect lines that come directly from the CO 208. After the system is installed, and with power off, the VPSTN 100 is transparent to the enterprise telecommunications system (i.e., all wire-pairs are terminated at the same points as prior to installation of the system).

[0055] Step 504 refers to userlist and group 406 configuration, discussed previously with reference to Figure 4 and later with reference to Figures 6A and 6B, whereby extensions are organized and labeled in relation to their commonality with other extensions as a means to "bundle" extensions together for convenience in managing telephony resources and

applying the security policy 302. As discussed previously with reference to Figure 4, other lists and groups may be created at this time, designating objects such as static secret keys, key exchange mechanisms, and encryption algorithms.

[0056] Step 506 refers to configuration of the security rule base 402, discussed previously with reference to Figure 4 and later with reference to Figures 7A-7B. Step 508 refers to configuration of the result response policy 404, discussed previously with reference to Figure 4 and later with reference to Figures 8A-8C. Steps 510-520 refer to the process of detecting call attributes and analyzing call activity, whereupon actions are taken for each call pursuant to the security policy 302, discussed below and in further detail later with reference to Figures 9A and 9B.

[0057] In Figure 5A, the process of call detecting and analyzing call activity begins in step 510. For each end-user station 136 connected by an individual station extension 152, direct connect line, or DS-1 circuit through the TA 102, the TA 102 will capture and analyze call activity, then consolidate and report details of the activity for further processing.

[0058] An aspect of this process involves the ability of the TA 102 to distinguish between voice, fax, modem, and VTC call types. Algorithms for call type distinction are utilized that, in one implementation, distinguish the call type based upon spectral analysis associated with typical fax and other data transmission protocols.

[0059] In step 512, a determination is made by the TA 102 as to what actions the security rule base 402 dictates to be taken for a particular call, depending upon the attributes

of the call, as determined in step 510. The rule-set for the security rule base 402, previously configured in step 506 and used in step 512, is configured and programmed to meet the resource management and security needs of the enterprise, which may include allowing the call, in which case execution proceeds directly to step 518; denying the call, in which case execution proceeds to step 514. As previously mentioned, the VPSTN 100 may be combined with a telecommunications firewall, resulting in a mixture of capabilities from each device; such as content monitoring, redirecting, recording, and authorizing remote access for the call; in which case execution proceeds to step 516.

[0060] In Figure 5B, in step 518, a determination is made whether the security rule base 402 also dictates track actions to be executed in step 520. If a negative determination is made, execution proceeds to step 510, as the VPSTN 100 continues detecting call attributes and analyzing call activity until the call ends. If a positive determination is made, execution proceeds to step 520 where the management server 106 performs track functions such as logging the call event and generating electronic mail notification, pager alerting, console messaging, and SNMP trap notification. As discussed previously with reference to the call log 304 and Figure 3, the call log 304 for each call is generated to an administrator-designated level of detail, ranging from very brief to verbose.

[0061] In step 522, a determination is made whether the security rule base 402 dictates that the TA 102 conduct the call in secure mode. If a negative determination is made, execution proceeds to step 510. If a positive determination is made in step 522, the

TA 102 conducts, or attempts to conduct the call in secure mode in step 524.

[0062] In step 526, the TA 102 evaluates the success or failure of the attempt in step 524 to conduct the call in secure mode against the result response policy 404 rule-set, thereby determining if additional actions or track functions are designated. For example, in response to a successful or failed attempt to setup and conduct a call in secure mode, the result response policy 404 may dictate responses such as: allowing or denying the call; sending a tone or message to indicate the call is secure or non-secure; logging the call event; sending notifications such as electronic mail notification, pager alerting, console messaging, or SNMP trap notification to designated system or security personnel; generation of a scheduled report; and automatic adjustment to the contents of groups 406 (and hence to the security policy 302); as described in step 528 and in further detail later with reference to Figures 8A-8C.

User List and Group Configuration

[0063] Figures 6A and 6B collectively illustrate a portion of the exemplary user and group listing 406, previously mentioned with reference to Figure 4 and step 504 in Figure 5A. The group listing 406 shown in Figures 6A and 6B defines each extension or direct connect line relative to its commonality with other extensions and lines, thereby "bundling" extensions together by commonality for convenience in managing telephony resources and applying the security policy 302. The security rule base 402 and result response policy 404

may refer to individual extensions, or may use group names to refer to all extensions in the group.

[0064] For example, all telephone extensions within the facility in the San Antonio offices which are intended to receive only voice calls, are listed in the "voice-only" group (i.e., extensions within the "sales," "engineering voice," "exec staff voice," and the "accounting voice" subgroups). All lines and extensions within the facility in the San Antonio offices which are intended to receive only fax calls, are listed in the "fax-only" group (i.e., several ungrouped fax extensions, and extensions within the "engineering fax" and the "exec staff fax" subgroups). All lines and extensions in the San Antonio offices with known and security configuration-approved modems are listed in the "authorized modem" group, which includes the "daily receivable modem" group, the "engineering modem" group, and several other authorized, individual modem extensions. The "inter-branch" group contains "branch offices voice-only," "branch offices fax-only," "branch offices authorized modem," and "branch offices video" subgroups from each branch office within the globally distributed organization, including the facility represented by the other groups listed within group 406. The group "*XXX**" is created to apply the security policy 302 to calls to and from a certain country (e.g., Country *X*), whereas "*XXX**" refers to the country code "*XXX*" for Country *X*, followed by any other number "*," thereby applying the security policy 302 against calls to a certain destination or from a certain source identified by a digital sequence. The VPSTN non-secure group contains certain lines and extensions on which secure calls

are expected to be conducted but could not be set up or conducted and on which all future calls are denied pending further investigation by security personnel.

Security Rule Base Configuration

[0065] Figures 7A and 7B collectively illustrate a portion of an exemplary security rule base, such as the security rule base 402, for use in connection with the VPSTN 100, as previously mentioned with reference to Figure 4, and step 506 in Figure 5A. Configuring the security rule base 402 involves creating a rule-set that defines what actions and track functions will be associated with particular groups of objects.

[0066] Referring to Figures 7A-7B, an example security rule base 402 defines rules that, based upon call attributes including "Direction" (inbound, outbound), "Source," "Destination," "Call type" (e.g., voice, fax, modem, VTC), "Date," "Time," and "Duration"(not shown), implement an "Action" (allow or deny the call), other additional actions, and logging, reporting and notification functions, "Track". Additionally, each rule has the TA 102 deployment location/identifier "Install On," allowing an enterprise to implement one single security rule base 402 containing rules designated to be applied in specific locations.

[0067] It is understood that the security rule base 402 may include any number and types of rules, and although not all possible call attributes are used in this example, rules may be constructed using any call attributes contained in the call log 304, as shown and described

with reference to Figure 3 and any objects or groups of objects as described with reference to Figures 4, 6A, and 6B.

[0068] Additionally, any combination of action(s) or tracking function(s) may be included in the security rule base 402, pursuant to the enterprise's telephony security and resource management needs.

[0069] It is further understood that each rule is evaluated in sequential order, and the security rule base 402 is exited after any one rule matches the determined call attributes. Because call-type detection is continuous during the call, change in call-type during a call is detected. Consequently, each rule in the security rule base 402, except for the rule already fired by the call's previous attribute, is re-evaluated in sequential order, using the updated call-type attributes. Actions and track functions are then performed based upon the rule matched with the updated call attribute.

[0070] Referring now to Figures 7A-7B, the Security Rule Base (SRB) 402 Rules 1-10 are explained as follows:

Rule 1:

[0071] This rule states "Deny outbound calls from extensions in the VPSTN non-secure group, generate an electronic mail and page, and log the call." This rule is installed on all TA 102. This rule identifies and segregates lines, and denies calls over the lines that are in the VPSTN non-secure group, and logs the call for accounting purposes.

Rule 2:

[0072] This rule states "Deny inbound calls to extensions in the VPSTN non-secure group, generate an electronic mail and page, and log the call." This rule is installed on all TA 102. This rule identifies and segregates lines, and denies calls over the lines that are in the VPSTN non-secure group, and logs the call for accounting purposes.

Rule 3:

[0073] This rule states "Allow inbound fax calls to extensions in the fax group between 9pm and 6am, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all inbound fax calls to extensions in the fax group during a specified time to be conducted in secure mode, and logs the call for accounting purposes.

Rule 4:

[0074] This rule states "Allow inbound modem calls to extensions in the daily receivable modem group, conduct the call in secure mode, and log the call." This rule is installed on the TA 102 in San Antonio. This rule causes all inbound modem calls to a specified inbound destination to be conducted in secure mode and logs the call for accounting purposes.

Rule 5:

[0075] This rule states "Allow all outbound international voice, fax, modem, and VTC calls to Country *X*, conduct the call in secure mode, and log the call." Note that the "*XXX**" in the "Destination" column represents any call with the country code for Country *X*,

"XXX" followed by any other number "*". This rule is installed on all TA 102. This rule causes all outbound voice, fax, modem, and VTC calls to any destination within Country *X* to be conducted in secure mode, and logs the call for accounting purposes.

Rule 6:

[0076] This rule states "Allow all inbound international voice, fax, modem, and VTC calls from Country *X*, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all inbound voice, fax, modem, and VTC calls from any inbound source within Country *X* to be conducted in secure mode, and logs the call for accounting purposes.

Rule 7:

[0077] This rule states "Allow inbound and outbound voice, fax, modem, and VTC calls between extensions in the inter-branch groups, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all inbound and outbound voice, fax, modem, and VTC calls to and from specified sources and destinations to be conducted in secure mode, and logs the call for accounting purposes.

Rule 8:

[0078] This rule states "Allow outbound voice, fax, modem, and VTC calls from extensions in the exec staff and engineering groups, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all outbound voice, fax,

modem, and VTC calls from specified outbound sources to be conducted in secure mode, and logs the call for accounting purposes.

Rule 9:

[0079] This rule states "Allow inbound voice, fax, modem, and VTC calls to extensions in the exec staff and engineering groups, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all inbound voice, fax, modem, and VTC calls to specified inbound destinations to be conducted in secure mode, and logs the call for accounting purposes.

Rule 10:

[0080] This catch-all rule states "Deny all calls, generate an electronic mail and log the call." This rule is installed on all TA 102. At first glance, this rule seems to deny any call to or from anywhere. This is not the case. This rule is typically placed at the bottom of the sequential list of rules to deny, log, and send notification for all calls that do not fit into any of the preceding rules. Again, each rule is evaluated in sequential order, exiting immediately after any one rule matches all the call attributes.

Security Policy – Result Response Policy Configuration

[0081] Figures 8A, 8B, and 8C collectively illustrate a portion of an exemplary result response policy, such as the result response policy 404, for use in connection with the VPSTN 100, as previously mentioned with reference to Figure 4, and step 508 in Figure 5A.

Configuring the result response policy 404 involves creating a set of response rules that define what action(s) and track functions(s) the TA 102 and the management server 106 perform responsive to attempted actions such as the success or failure of initiating and conducting a secure call.

[0082] Referring to Figures 8A-8C, an example result response policy 404 defines rules that, based upon the extension's "Current Group," "Call type" (e.g., fax, modem, voice, VTC), the "Attempt" that was made pursuant to the fired security rule base 402 rule, and the "Result" of the attempt, implements an "Action" (allow or deny the call), notification and event logging functions ("Track"), an option to automatically adjust the security policy 302 ("Adjust Policy"), and defines the new group the extension will be placed in ("Move To"). Additionally, each rule has a deployment location "Install On," allowing an enterprise to implement one single result response policy 404 containing rules designated to be applied in specific TA locations.

[0083] It is understood that the result response policy 404 may include any number and types of rules, and although not all possible call attributes are used in this example, rules may be constructed using any call attributes contained in the call log 304, as shown and described with reference to Figure 3 and any objects or groups of objects as described with reference to Figures 4, 6A, and 6B.

[0084] Additionally, any combination of action(s) or tracking function(s) may be included in the result response policy 404, pursuant to the enterprise's telephony security and resource management needs.

[0085] It is further understood that each rule is evaluated in sequential order, and the result response policy 404 is exited after any one rule matches the determined call attributes.

[0086] Referring now to Figures 8A, 8B, and 8C, the Result Response Policy (RRP) 404 Rules 1-9 are explained as follows:

Rule 1:

[0087] This rule states "Allow inbound fax calls to extensions in the fax-only group that are successfully conducted in secure mode and log the event;" and

"Deny inbound fax calls to extensions in the fax-only group that fail to be conducted in secure mode, play a tone, generate an electronic mail, and log the event."

This rule is installed on all TA 102. This rule allows secure fax communication and denies all non-secure fax communication with extensions in the fax-only group. This result response policy rule is applicable to security rule base 402 Rule 3 of Figure 7A.

Rule 2:

[0088] This rule states "Allow inbound modem calls to extensions in the daily receivable group that are successfully conducted in secure mode and log the event;" and

"Deny inbound modem calls to extensions in the daily receivable group that fail to be conducted in secure mode, play a tone, generate an electronic mail, a page alert, log the

event, and move the daily receivable modem extension from the daily receivable modem group to the VPSTN non-secure group."

This rule is installed on all TA 102. This rule allows secure inbound modem communication with extensions in the daily receivable group and denies all non-secure communication. Failure to conduct a secure call within the enterprise may be a result of packet tampering, so the line is moved to the VPSTN non-secure group, denying further use. Designated personnel are notified via electronic mail and pager for investigation and follow-up. This result response policy rule is applicable to security rule base 402 Rule 4 of Figure 7A.

Rule 3:

[0089] This rule states "Allow voice and VTC calls to and from Country *X* that are successfully conducted in secure mode, play a tone, and log the event;" and

"Deny voice and VTC calls to and from Country *X* that fail to be conducted in secure mode, play a message, generate an electronic mail, and log the event."

This rule is installed on all TA 102. This rule allows secure voice and VTC communication with Country *X*, and denies all non-secure communication with an audible warning if secure communication is not possible. This result response policy rule is applicable to security rule base 402 Rules 5 and 6 of Figures 7A and 7B.

Rule 4:

[0090] This rule states "Allow fax and modem calls to and from Country *X* that are

successfully conducted in secure mode and log the event;" and

"Deny fax and modem calls to and from Country *X* that fail to be conducted in secure mode, play a tone, generate an electronic mail, and log the event."

This rule is installed on all TA 102. This rule allows secure fax and modem communication with Country *X*, and denies all non-secure communication with a warning tone if secure communication is not possible. This result response policy rule is applicable to security rule base 402 Rules 5 and 6 of Figures 7A and 7B.

Rule 5:

[0091] This rule states "Allow voice and VTC calls between extensions in the inter-branch group that are successfully conducted in secure mode, and log the event;" and

"Deny voice and VTC calls between extensions in the inter-branch group that fail to be conducted in secure mode, play a message, generate an electronic mail, and log the event."

This rule is installed on all TA 102. This rule allows only secure voice and VTC communication between extensions in the inter-branch group and denies all non-secure communication. This result response policy rule is applicable to security rule base 402 Rule 7 of Figure 7B

Rule 6:

[0092] This rule states "Allow fax and modem calls between extensions in the inter-branch group that are successfully conducted in secure mode and log the event;" and

"Deny fax and modem calls between extensions in the inter-branch group that fail to

be conducted in secure mode, play a tone, generate an electronic mail, and log the event."

This rule is installed on all TA 102. This rule allows secure fax and modem communication between extensions in the inter-branch group, and denies all non-secure communication. This result response policy rule is applicable to security rule base 402 Rule 7 of Figure 7B.

Rule 7:

[0093] This rule states "Allow voice and VTC calls to and from extensions in the exec staff and engineering groups that are successfully conducted in secure mode and log the event;" and

"Allow voice and VTC calls to and from extensions in the exec staff and engineering groups that fail to be conducted in secure mode, play a message, generate an electronic mail, and log the event."

This rule is installed on all TA 102. This rule allows secure voice and VTC communication with extensions in the exec staff and engineering groups, and allows non-secure communication with an audible warning if secure communication is not possible. This result response policy rule is applicable to security rule base 402 Rules 8 and 9 of Figure 7B.

Rule 8:

[0094] This rule states "Allow fax and modem calls to and from extensions in the exec staff and engineering groups that are successfully conducted in secure mode and log the

event;" and

"Allow fax and modem calls to and from extensions in the exec staff and engineering groups that fail to be conducted in secure mode, sound a tone, and log the event."

This rule is installed on all TA 102. This rule allows secure fax and modem communication with extensions in the exec staff and engineering groups, and allows non-secure communication with a warning tone if secure communication is not possible. This result response policy rule is applicable to security rule base 402 Rules 8 and 9 of Figure 7B.

Rule 9:

[0095] This catch-all rule states "Deny all calls, generate an electronic mail, and log the call." This rule is installed on all TA 102. At first glance, this rule seems to deny any call from anywhere. This is not the case. This rule is typically placed at the bottom of the sequential list of rules to deny, log, and send a notification for all calls that do not fit into any of the preceding rules. Again, each rule is evaluated in sequential order, exiting immediately after any one rule matches all the call attributes.

Security Policy – "Secure All Possible Calls" Configuration

[0096] Figures 8D and 8E collectively illustrate an alternate security policy 416 for the VPSTN 100 wherein a security rule base 412 and a result response policy 414 promote secure communication with any VPSTN-capable source or destination. As shown in Figure 8D, the security rule base 412 consists primarily of one "Secure All Possible Calls" rule

which states "Allow calls from any direction (inbound and outbound), from any source, to any destination, of any call type, on any date, at any time, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. Alternatively, it is contemplated that an organization may want to promote secure communication and yet may need to refrain from using the VPSTN 100 secure communications on specific extensions or on calls with specific attributes (e.g., STE calls). In such a case, the current Rule 1 in Figure 8D is preceded by rules configured to address these specific needs.

[0097] Figure 8E shows the result response policy 414 for the security rule base 412 of Figure 8D. The result response policy 414 consists primarily of one rule which states "Allow calls with any extension that is successfully conducted in secure mode and log the event;" and "Allow calls with any extension that fails to be conducted in secure mode, sound a tone, and log the event." It is understood that, if desired, Rule 1 can be configured such that calls are denied if the attempt to conduct the call in secure mode fails. Alternatively, it is contemplated that an organization may want to promote secure communication and yet may need to allow or deny a call based on the success or failure to conduct the call in secure mode and at least one other call attribute (e.g., the current group, call type, etc.). In such a case, the current Rule 1 in Figure 8E is preceded by rules configured to address these specific needs.

Security Rule Base Enforcement

[0098] Figures 9A and 9B collectively illustrate a process flow diagram 900 whereby

detection and analysis of call activity and implementation of the security rule base 402 are executed by the VPSTN 100, as previously mentioned with reference to steps 510-528 of Figures 5A and 5B. In Figure 9A, steps 912-946 illustrate that the TA 102 captures and analyzes all available call attributes, analyzes call-activity, and then consolidates and reports details for further processing.

[0099] In particular, in step 912, call-progress signals on the line are captured and analyzed and a determination is made whether the call is an inbound call in step 914. If so, execution proceeds to step 916, in which the destination is set equal to the line map (i.e., the mapping of the individual station extensions 152 through the TA 102) so that the destination extension can be determined according to the line map, and the source is set equal to caller-ID (so that a caller identification device determines the source of the inbound call). In step 918, the available caller-ID or ANI information is decoded and recorded, and execution proceeds to step 930.

[0100] Referring again to step 914, if a negative determination is made (i.e., that the call is not an inbound call), execution proceeds to step 920, in which a determination is made whether the call is an outbound call. If a negative determination is made, execution proceeds to step 922, in which an exception is characterized in the call-event record. If the call is determined to be outbound, execution proceeds to step 924, in which the source is set equal to the line map (so the extension from which the call is made can be identified), and the destination is set equal to the dialed digits (indicating that the TA 102 determines the

destination of the call). In step 926, the DTMF/MF signals are decoded and recorded to determine the number that was dialed, and execution proceeds to step 930.

[0101] In step 928, a determination is made whether the currently determined call attributes (call direction, source, destination, etc.) match the security rule base 402 rule criteria. If so, execution proceeds to step 930, in which the action and track functions associated with the matched security rule base 402 rule, such as initiating secure mode, are initiated.

[0102] In step 931, handshake signals are captured and analyzed, and data is demodulated in the case of both inbound and outbound calls for use in discriminating the call type of the call to be video, fax, modem, or voice in steps 932-944. In step 932, a determination is made whether the call is video, and if so, execution proceeds to step 934, in which the call-type of "video" is assigned to the call. If the determination in step 932 is negative, execution proceeds to step 936.

[0103] In step 936, a determination is made whether the call is fax, and if so, execution proceeds to step 938, in which the call type of "fax" is assigned to the call. If the determination in step 936 is negative, execution proceeds to step 940.

[0104] In step 940, a determination is made whether the call is modem, and if so, execution proceeds to step 942, in which the call-type of "modem" is assigned to the call. If the determination in step 940 is negative, execution proceeds to step 944 where the call type of "voice" is assigned to the call.

[0105] Upon completion of step 922, 934, 938, 942, or 944, execution proceeds to step 946, wherein all available call attributes (e.g., the call direction, source number, destination number, trunk group, trunk, channel ID, and call type), are consolidated in a concatenated call event record for use in implementing the security rule base 402. From step 946, execution proceeds to step 948 (Figure 9B).

[0106] Referring now to Figure 9B, in step 948, the TA 102 compares the determined call attributes within the call event record with rules in the security rule base 402. Rules are evaluated for a call event in sequential order. Steps 950-966 illustrate a process loop that is applied for each rule until either one rule's criteria meets the determined call attributes and an action is indicated for the current rule in step 964, or not all designated attributes in a rule (and hence no rule) meets the determined call attributes. The call attributes may include, but are not limited to, any Boolean combination (AND, OR, NOT) of the following: (1) direction of the call (i.e., inbound or outbound); (2) source telephone number, numbers, or mask (e.g., 210-402-XXXX) where the source number is the number of the party initiating the call (i.e., the extension assigned to a station for outbound calls, or the number extracted from caller-ID or any other means for inbound calls); (3) destination telephone number, numbers, or mask where the destination number is the number of the party receiving the call (i.e., the extension assigned to a station for inbound calls, or the number dialed, DTMF decoded or by any other means for outbound calls); (4) type of call, defined as either voice, fax, modem, or video; (5) date of call, defined as specific dates,

ranges of dates, day(s)-of-week, or any combination thereof; (6) time of call, defined as specific times, ranges of times, time(s)-of-day, or any combination thereof; (7) the deployment location/identifier of the TA 102; and (8) any other call attribute listed with reference to the call log 304.

[0107] In particular, in step 952, a determination is made whether the call direction matches the rule criteria. If so, execution proceeds to step 954, in which a determination is made whether the source matches the rule criteria. If so, execution proceeds to step 956, in which a determination is made whether the destination matches the rule criteria. If the destination matches the rule criteria, execution proceeds to step 958, in which a determination is made whether the call type matches the rule criteria. If so, execution proceeds to step 960, in which a determination is made whether the date and time fall within the rule criteria. If so, execution proceeds to step 962, in which a determination is made whether the deployment location/identifier of the TA 102 (through which the call flows), matches the "install on" rule criteria. If the "install on" rule criteria matches the TA 102 deployment location/identifier, execution proceeds to step 964, in which the action and track functions associated with the matched security rule base 402 rule are initiated.

[0108] When the criteria of the security rule base 402 rule is matched, the TA 102 performs actions and track functions dictated by the rule in step 964, which may include: allow or deny the call and conduct the call in secure mode. The TA 102 notifies the management server 106 that the security rule base 402 rule has fired. The management

server 106 references the fired security rule base 402 rule and performs track functions dictated by the rule, which may include: send notifications such as electronic mail notification, pager alerting, console messaging, or a SNMP trap notification, and logging the event.

[0109] Detection and analysis of call activity and implementation of the security rule base 402 is completed in step 968, however, it is understood that call activity is monitored and analyzed during the life of the call. It is further understood that each security rule base 402 rule is evaluated in sequential order, and the security rule base 402 is exited after any one rule matches the determined call attributes. Although not shown, if the TA 102 or TA 104 detects a change in the call attributes or detects additional call attributes (not available at the time the rule requiring secure mode fired), each rule in their respective security rule base 402, except for the rule already fired by the call's previous attributes, is re-evaluated in sequential order, using the updated attributes. Actions and track functions are then performed based upon the rule matched with the updated call attribute.

[0110] Referring again to step 952, 954 ,956, 958, 960, and 962, if a negative determination is made in one of these steps, execution proceeds to step 966, in which a determination is made whether the current rule is the last rule to be evaluated. If not, execution returns to step 950 and the next rule is retrieved; otherwise, execution terminates in step 968.

Result Response Policy Enforcement

[0111] Figures 10A and 10B collectively illustrate a process flow diagram 1000 whereby evaluation of the results (success or failure) of the secure call attempt, and implementation of the result response policy 404, are executed by the VPSTN 100, as previously mentioned with reference to step 524-528 of Figure 5B. In Figures 10A and 10B, steps 1002-1014 illustrate that the TA 102 applies a process loop, evaluating each result response policy 404 rule in sequential order until either one rule matches all designated attributes of the call and the attempt result, or no rule meets all criteria. It is understood that the VPSTN 100 is capable of operating in a continuous loop, initiating and executing secure calls while simultaneously performing appropriate actions pursuant to the security rule base 402 and result response policy 404.

[0112] Now referring to step 1002 in Figure 10A, the TA 102 compares the result (success or failure) of the attempt to conduct the call in secure mode and the determined call attributes with the rules in the result response policy 404. The rule criteria may include, but is not limited to any Boolean combination (AND, OR, NOT) of the following: (1) current group, defined as the user group in which the inbound or outbound telephone number or extension is currently listed; (2) call type, defined as either voice, fax, modem, or video; (3) attempt, defined as the action or track function to be attempted, pursuant to the fired security rule base 402 rule (e.g., conducting the call in secure mode); (4) result, defined as the successful or failed execution of the attempted action or track function; (5) the deployment

location/identifier of the TA 102; and (6) any other call attribute listed with reference to the call log 304.

[0113] In particular, in step 1004, a determination is made whether the call extension or the current group containing the call extension matches the rule criteria. If so, execution proceeds to step 1006, in which a determination is made whether the call type matches the rule criteria. If the call type attribute of the call matches the rule criteria, execution proceeds to step 1008. In step 1008, a determination is made whether the attempt made by the TA 102 (e.g. conduct the call in secure mode), matches the rule criteria. If so, execution proceeds to step 1010, in which a determination is made whether the result of the attempt (e.g. success or failed), matches the rule criteria. If so, execution proceeds to step 1012, in which a determination is made whether the TA 102 location/identifier matches the "install on" rule criteria. If so, execution proceeds to step 1016.

[0114] In step 1016, a determination is made whether the matched result response policy 404 rule dictates adjustment of the security policy 302. If so, execution proceeds to step 1018, in which the management server 106 moves the extension from its current designated group into a different, designated group, and execution proceeds to step 1020. If the security policy is adjusted, in step 1020, the management server 106 synchronously downloads the updated security policy 302 to any TA 102 that is designated to use that specific security policy 302 (shown in the "install on" column). In step 1022, the action(s),

track function(s) and/or additional action(s) associated with the fired result response policy 404 rule are performed. Execution is complete in step 1024.

[0115] Referring again to steps 1004, 1006, 1008, 1010, and 1012, if a negative determination is made in any of these steps, execution proceeds to step 1014, in which a determination is made whether the current rule is the last rule to be evaluated in the result response policy 404. If not, execution returns to step 1002 and the next rule is retrieved for comparison; otherwise, execution is completed in step 1024.

The VPSTN DS-0 Channel Sample

[0116] The DS-0 channel is the atomic level (the lowest level) of a standard telephony call, regardless of whether the call is voice, fax, modem, or VTC. As previously mentioned, the DS-0 channel operates at 64,000 bps. The VPSTN 100 subdivides the VPSTN DS-0 channel sample into subrate channels. The term subrate is used because each of the channels operate below the full DS-0 channel rate. The subrate channels are assigned bit positions within the VPSTN DS-0 channel sample, as discussed with reference to Figures 11A, 11B, and 11C. It is understood that multiple embodiments of subrate channel locations and size (bit assignments) are possible, subdividing the VPSTN DS-0 channel sample into two or more subrate channels based on various factors such as DS-1 type, channel impairments, the designated encryption algorithm and encryption engine, compression algorithms, etc.

[0117] Based on the type of DS-1 in which the TA is installed, as well as the enterprise's security needs, the system administrator will configure the TA to operate at select allowed secure modes represented by the VPSTN DS-0 channel samples discussed below with reference to Figures 11A, 11B, and 11C.

[0118] It is understood that secure modes for data calls may include, for example: unrestricted digital information at 64Kbps, restricted digital information at 64Kbps, unrestricted digital information at 56Kbps, and restricted digital information at 56Kbps. However, for simplicity, the explanations herein will deal with only two secure modes for data calls: unrestricted digital information at 64Kbps and unrestricted digital information at 64Kbps adapted to 56Kbps, referred to herein as data at 64Kbps and data at 56Kbps respectively.

[0119] It is further understood that voice call secure modes may include the following information transfer rates: 56Kbps, 48Kbps, 40Kbps, 32Kbps, and 24Kbps, and are referred to herein as voice at 56Kbps, voice at 48Kbps, voice at 40Kbps, voice at 32Kbps, and voice at 24Kbps, respectively.

[0120] Figure 11A is a schematic block diagram illustrating subrate channels and bit assignments in an exemplary VPSTN 100 DS-0 channel sample 1150 for data call secure mode at 64Kbps. The DS-0 channel sample 1150 is produced by the VPSTN 100 on a DS-1 such as an ISDN PRI trunk supporting data at 64Kbps.

[0121] The subrate channels include a control channel 1152 (sometimes called a

packet header, message, or synchronization channel), and a secured media channel 1154 (sometimes referred to as a subrate bearer, barrier, or packet payload channel). The secured media channel 1154 operates at a DS-0 subrate of 56,000 bps (7-bits per sample). The control channel 1152 operates at a subrate of 8,000 bps (1-bit per sample). The two subrate channels (the control channel and the secured media channel) add up to a rate of 64 (56 + 8) Kbps. The control channel 1152 is assigned bit position 0, which is the Least Significant Bit (LSB). The secured media channel 1154 is assigned bit positions 1, 2, 3, 4, 5, 6, and 7. Secure mode 64Kbps uses 7-bit PCM, although use of compression is contemplated to allow for increased throughput.

[0122] Figure 11B is a schematic block diagram illustrating subrate channels and bit assignments in an exemplary VPSTN 100 DS-0 channel sample 1160 for data call secure mode at 56Kbps and voice call secure mode at 56Kbps. The DS-0 channel sample 1160 is produced by the VPSTN 100 on a DS-1 such as an ISDN PRI trunk supporting data at 56Kbps; and a T1 with no line impairments.

[0123] The subrate channels include a control channel 1162, a secured media channel 1164, and a discarded channel 1166. The secured media channel 1164 operates at a DS-0 subrate of 48,000 bps (6-bits per sample). The control channel 1162 operates at a subrate of 8,000 bps (1-bit per sample). The discarded channel contains the LSB (bit position 0). The two subrate channels add up to a rate of 56 (48 + 8) Kbps. The control channel 1162 is assigned bit position 1. The secured media channel 1164 is assigned bit

positions 2, 3, 4, 5, 6, and 7. Data call secure mode at 56Kbps and Voice call secure mode at 56Kbps uses 6-bit PCM, although use of compression is contemplated to allow for increased throughput.

[0124] In data call secure mode, using VPSTN DS-0 channel samples 1150 and 1160, the VPSTN 100 sends voice calls across the PSTN 116 as a data call, so network echo suppressors, digital pads, and other digital impairments are not present and therefore do not have to be disabled or taken into account when transmitting data.

[0125] Figure 11C is a schematic block diagram illustrating subrate channels and bit assignments in an exemplary VPSTN 100 DS-0 channel sample 1170 for voice call secure mode at 48Kbps. The DS-0 channel sample 1170 is produced by the VPSTN 100 on a DS-1 such as T1 trunks with line impairments.

[0126] The subrate channels include a control channel 1172, a secured media channel 1174, and a discarded channel 1176. The secured media channel 1174 operates at a DS-0 subrate of 40,000 bps (5-bits per sample). The control channel 1172 operates at a subrate of 8,000 bps (1-bit per sample). The discarded channel contains the LSB (bit position 0) and bit position 1. The two subrate channels add up to a rate of 48 (40 + 8) Kbps. The control channel 1172 is assigned bit position 7, which is the Most Significant Bit (MSB). The secured media channel 1174 is assigned bit positions 2, 3, 4, 5, and 6. Voice call secure mode at 48Kbps uses ADPCM in 5-bit mode for compressing the 8-bit data stream.

[0127] Although not shown, it is contemplated that the VPSTN 100 will also operate in voice call secure modes on DS-1s such as T1 trunks supporting less than 48Kbps information transfer rates, specifically on trunks supporting 40Kbps, 32Kbps, and 24Kbps. For example, the VPSTN DS-0 channel sample for voice call secure mode at 40Kbps is made up of a subrate control channel operating at a subrate of 8,000 bps (1-bit per sample), a secured media channel operating at a DS-0 subrate of 32,000 bps (4-bits per sample). A discarded channel contains the LSB (bit position 0) and bit position 1 and 2. The two subrate channels add up to a rate of 40 (32 + 8) Kbps. The secured media channel is assigned bit positions 3, 4, 5, and 6, and the control channel is assigned bit 7. Voice call secure mode at 40Kbps uses ADPCM in 4-bit mode for compressing the 8-bit data stream.

[0128] VPSTN DS-0 channel samples for voice call secure mode at 32Kbps, and voice call secure mode at 24Kbps are similarly constructed as those previously described, such that the control channel is assigned bit 7 and operates at a subrate of 8,000 bps (1-bit per sample). For voice call secure mode at 32Kbps: the secured media channel operates at a DS-0 subrate of 24,000 bps (3-bits per sample) and is assigned bit positions 4, 5, and 6; voice call secure mode at 32Kbps uses ADPCM in 3-bit mode for compressing the 8-bit data stream; the discarded channel contains the LSB (bit position 0) and bit positions 1, 2, and 3; therefore the two subrate channels add up to a rate of 32 (24 + 8) Kbps. For voice call secure mode at 24Kbps: the secured media channel operates at a DS-0 subrate of 16,000 bps (2-bits per sample) and is assigned bit positions 5 and 6; voice call secure mode at 24Kbps uses

ADPCM in 2-bit mode for compressing the 8-bit data stream; the discarded channel contains the LSB (bit position 0) and bit positions 1, 2, 3, and 4; therefore the two subrate channels add up to a rate of 24 (16 + 8) Kbps.

[0129] Figure 11D is a schematic block diagram illustrating an example structure of the VPSTN 100 DS-0 packet made up of VPSTN DS-0 channel samples 1150, 1160, 1170, or those samples discussed above, but not show-n. The VPSTN DS-0 packet is configured such that it can be transmitted and received over either the circuit switched PSTN 116 or a packet switched network to support secure voice over IP (VoIP). The packet header 1182 is further subdivided into 3 fields: a synchronization/message field 1188; a status word 1190, and an Initialization Vector (IV) field 1192.

[0130] The 32-bit status word field 1190 is used to transmit control data from the TA 102 to the TA 104, and vice versa. The bit-0 within the status word field 1190 indicates if encryption is enabled for that particular channel. If the TA 102 or 104 receives a packet wherein bit-0 within the status word field 1190 is set to 1, then the VPSTN DS-0 packet is indicated to contain an encrypted payload in secured media 1184 and decryption is required. Conversely, if bit-0 within the status word field 1190 is set to 0, the packet contains plaintext data and decryption is not necessary. Any set of bits or bit fields may be used to exchange control or status information between the TA 102 and the TA 104.

[0131] The synchronization/message field 1188 is used to pass messages between the TA 102 and the TA 104. Messages are used to setup a secure call, exchange and negotiate

TA capabilities, exchange encryption keys, report errors, and control the call session. The synchronization/message field 1188 remains active throughout the duration of a call, and is used to initiate or discontinue secure mode while a call is in progress.

[0132] The synchronization (sync)/message field 1188 is used to transmit a fixed bit synchronization pattern, thereby providing a means for delineating the boundaries of the VPSTN DS-0 packet. The VPSTN DS-0 packet boundary is not related to the framing performed by the PSTN 116, such as the D3/D4 framing or Extended Super Frame (ESF) formats. Since the probability that a non-VPSTN 100 device would randomly produce the synchronization pattern is very low, the pattern is also used to identify or confirm that the VPSTN DS-0 packet was transmitted by a VPSTN-capable TA 102 or 104.

[0133] It is contemplated that the synchronization/message field 1188 may be used to monitor the time that it takes for VPSTN DS-0 packets 1180 to reach the other TA and return. If the timing for a "round trip" is not consistent throughout the length of the call, "man-in-the-middle" tampering, or re-routing of the circuits within the PSTN 116 may be indicated.

[0134] The Initialization Vector (IV) field 1192 is used to transport encryption algorithm parameters, such as modulus length, crypto seed, and exponents. When using the DES or 3-DES encryption algorithm, the IV field 1192 is used to initialize the algorithm with random data to perform the encryption.

[0135] The payload field 1194 may carry the channel data in a compressed format,

depending on the secure mode being used. It will be understood by those skilled in the art that a wide range of compression methods may be applied, but the ITU-T G.726 Recommendation, Adaptive Differential Pulse Code Modulation (ADPCM) in 5-bit mode is the preferred method for compressing the 8-bit Pulse Code Modulated (PCM) audio data, since ADPCM 5-bit mode (which operates at 40K bps), provides voice quality equal to that of an uncompressed PCM DS-0 channel at 64 Kbps (i.e., toll quality).

[0136] Figure 12 is a process flow diagram illustrating the process 1200 whereby the VPSTN 100 conducts a voice call in secure mode. In step 1202, (reference will also be made to the elements within Figure 1 for this example), the PSTN 116 uses normal, non-secure telecommunications processes for connecting two terminals (e.g., telephone sets 148 calls telephone set 150). Responsive to the firing of the security rule base 402 rule requiring secure communication, the TA 102 and the TA 104 either intercepts and alters the call setup message (ISDN PRI trunks) or allows the call to be connected, then performs autodiscovery, synchronization, and capabilities negotiation processes. If the TA 102 is installed in an ISDN PRI trunk and monitoring the Data (D) channel, the call setup process described with reference to Figures 13A-13B is executed. If the TA 102 is installed in a T1 trunk, the call setup process described with reference to Figures 13C-13E, is executed. It is understood by those skilled in the art that instances wherein the TA 102 or TA 104 are installed in "ISDN-like" (such as E1, SS7, or J1 trunks) or "T1-like" trunks, either: the process described with reference to Figures 13A-13B related to ISDN PRI trunks, the process described with

reference to Figures 13C-13E related to T1 trunks, or a combination of portions of both processes will be used.

[0137] The session's secret key is established between the TA 102 and the TA 104 in step 1204. Various administrator-designated session keys and exchange methods are contemplated, including static keys, shared secret keys, Public Key Exchange (PKE)-transmitted session keys, digital certificates, or other key exchange mechanisms. In the case of static keys, no key exchange is required. Key exchange is performed in the synchronization/message field 1188 (Figure 11D). In the preferred embodiment, each call (session) has two unique secret keys. The TA 102 and the TA 104 each transmit their data key using PKE, thereby creating a unique session key for each transmit channel. Following establishment and exchange of the session keys, in step 1206 the TA 102 and the TA 104 begin encrypting the payload 1194 (Figure 11D).

[0138] In step 1206, the TA 102 PBX-in port 120 receives the non-secure DS-1 circuit data from the PBX 114. The TA 102 may compress the circuit data (if required by the DS-1 line type and the secure mode level) and encrypts the non-secure data bit stream, thereby generating the secure VPSTN DS-0 channel sample 1150 bit stream. The TA 102 PSTN-out port 122 transmits the secured DS-0 bit stream to the PSTN 116, where it is switched to the PBX 118.

[0139] In step 1208, the TA 104 PSTN-in port 128 receives the secured DS-0 bit stream from the PSTN 116. The TA 104 decrypts and decompresses (if required) the secure

data stream, thereby restoring the non-secure data bit stream that was previously compressed (if required) and encrypted in step 1206. The TA 104 PBX-out port 130 transmits the non-secure DS-1 circuit data stream to the PBX 118, which transmits the signal to the telephone 150.

[0140] While not shown, it is understood that the VPSTN 100 is capable of operating in a continuous loop, synchronously handling the flow of both the receiving and transmitting DS-0 channel data streams. The process loop continues until the call is "hung up." The PSTN 116 tearsdown the call using normal telecommunications processes for disconnecting the two phone sets 148 and 150, as shown in steps 1210 and 1212.

[0141] In step 1214, the call event is logged, and any other actions and track functions required by the security policy 302, such as generation of notifications are executed.

[0142] Figures 13A-13B collectively show a process flow diagram for the secure call setup and conduction process 1300, whereby secure mode capabilities between the call source TA 102 and the destination TA 104 are autonomously established on a DS-1 circuit including of ISDN PRI access trunks (reference will also be made to the elements in Figure 1 for this flowchart).

[0143] In step 1302, as an audio connection is being established between the telephone 148, PBX 114, PSTN 116, PBX 118, and the telephone 150 (using the normal,

non-secure method used for connecting two phone sets across the PSTN 116), the call setup message from the PBX 114 is received by the in-line TA 102.

[0144] It is understood that herein, reference to PBX 114 or PBX 118 may also refer to the end-user station 136 or 138 directly connected to the CO 208 or PSTN 116. Further, although the same numerals are used for reference, the security policy 302, security rule base 402, and result response policy 404 contained within the TA 102 and TA 104 may be the same or different.

[0145] In step 1304, the TA 102 collects and analyzes the call attributes that are available within and at the time of the call setup message (such as call direction, source, destination, etc.) , as previously mentioned with reference to steps 510-522 of Figures 5A and 5B and steps 912-964 of Figures 9A and 9B.. These determined call attributes are compared against the security rule base 402. In step 1306, the TA 102 determines if all of the determined call attributes match a security rule base 402 rule (such as the "Secure All Possible Calls" rule previously discussed with reference to Figure 8D), requiring the call to be conducted in secure mode. If the determination is negative, i.e., if no rule is matched in step 1304, or if a rule is matched that does not require the call to be conducted in secure mode, then the call will be conducted using the normal, non-secure method for conducting a call across the PSTN 116 in step 1308.

[0146] In step 1310, the TA 102 examines the setup message and determines whether the Bearer Capability Information Element (IE) contains a PBX 114 request for a voice call.

If a negative determination is made, that is, if the PBX 114 requests a data call, it is assumed that the call will require the full bearer capability of the channel and the call will not be conducted in secure mode, regardless of the fired security rule base 402 rule. Therefore, if a negative determination is made, the process proceeds to step 1308 and the secure call setup process 1300 is discontinued and the call will be conducted using the normal, non-secure method for conducting a call across the PSTN 116. However, if in step 1310, the TA 102 determines the setup message includes a request for a voice call, and a determination is made in step 1312 that the call is an outbound call, the process proceeds to step 1314.

[0147] In step 1314, the TA 102 alters the setup message prior to forwarding the message to the PSTN 116. The TA 102 changes the PBX 114 request (i.e., the call's request) in the Bearer Capability IE from a voice call request to a request for either an unrestricted or restricted data call at 64Kbps or an unrestricted or restricted data call at 64Kbps adapted to 56Kbps, or a restricted data call at 56Kbps, in accordance with the administrator-configured listing of allowed modes.

[0148] In step 1314, the TA 102 also adds or alters the User-to-User Information IE to include: (1) a codeword indicating that the TA 102 is VPSTN-capable and its security policy 302 dictates that this call is to be conducted in secure mode; (2) the original Bearer Capability IE; (3) the TA 102 secure mode capabilities; and (4) any other information appropriate to be communicated to the TA 104 at this time. It is understood that the TA 102 and TA 104 may use other IEs (such as the High Layer Compatibility IE, the Low Layer

Compatibility IE, or the Progress Indicator IE), to communicate the above described or other information.

[0149] In step 1316, the TA 102 forwards the altered setup message to the PSTN 116, thereby indicating (to the TA 104) the TA 102 secure mode capabilities and its readiness to conduct the call in secure mode at connect time. The TA 102 then waits to receive an acknowledging response from the TA 104 in the form of an altered alerting or connect message.

[0150] In step 1318, the TA 104 receives the altered setup message from the PSTN 116 and in step 1320, collects and analyzes the call attributes that are available within and at the time of the setup message. These determined call attributes are compared against the TA 104 security rule base 402. In step 1322, the TA 104 determines if all of the call attributes match a security rule base 402 rule requiring the call to be conducted in secure mode. If so, the process will proceed to step 1324. If no rule is matched in step 1320, or if a rule is matched that does not require the call to be conducted in secure mode, the call will be conducted using the normal, non-secure method for conducting a call across the PSTN 116 in step 1308.

[0151] In step 1324, the TA 104 checks the User-to-User Information IE for the codeword which indicates the call is from a VPSTN 100-capable source which is ready to conduct the call in secure mode at connect time. Note that prior to finding the codeword, the call appears to both the PSTN 116 and the TA 104 to be a typical data call at 64Kbps or

56Kbps. If the codeword is found, the process proceeds to step 1326. If the codeword is not found in the User-to-User Information IE, the TA 104 assumes the call is not a TA-requested data call, but is instead, a PBX-requested data call requiring the full capacity of the channel, so the process proceeds to step 1308 and the call will be conducted using the normal, non-secure method for conducting a call across the PSTN 116.

[0152] Having found the codeword in the User-to-User Information IE in step 1324, in step 1326, the TA 104 modifies the altered setup message received from the TA 102 by replacing the TA 102-altered Bearer Capability IE with the original Bearer Capability IE that was transmitted via the User-to-User Information IE. In step 1326, the TA 104 removes all information the TA 102 inserted into the User-to-User Information IE during step 1314, or removes the User-to-User Information IE completely if it only contained information from the TA 102. In step 1328, the TA 104 forwards the restored setup message to the PBX 118. The TA 104 then waits to receive an alerting or connect message from the PBX 118.

[0153] In step 1330, the TA 104 receives either an alerting message, connect message, or a release (end of call) message from the PBX 118. If a release message is received, the TA 104 forwards the message to the TA 102. However, if the TA 104 receives the alerting or connect message from the PBX 118, the TA 104 alters the alerting or connect message in step 1334 prior to forwarding the message to the PSTN 116.

[0154] In step 1334, the TA 104 adds or alters the User-to-User Information IE to include: (1) a codeword indicating that the TA 104 is VPSTN 100-capable and ready to

conduct the call in secure mode at connect time; (2) the TA 104 secure mode capabilities; and (3) any other information appropriate to be communicated to the TA 102 at this time. An example of other information that may be communicated using the User-to-User Information IE or other IEs is: when applicable, the TA 104 may use an IE to inform the TA 102 that the TA 104 security rule base 402 does not allow the call to be conducted in secure mode, in which case the TA 102 responds in accordance with the TA 102 result response policy 404, as discussed in step 1340. In step 1336, the TA 104 forwards the altered alerting or connect message to the PSTN 116, thereby providing to the TA 102 an acknowledging response and, as necessary, indication that a lower secure mode is required for the TA 104 to participate in the secure call process.

[0155] In step 1338, the TA receives either an altered alerting or connect message, or a release (end of call) message from the TA 104. If the TA 102 receives a release message, the TA 102 tearsdown the call and responds to the failure to setup a secure call in step 1340, pursuant to the TA 102 result response policy 404.

[0156] In step 1340, responses by the TA 102 and management server 106 in accordance with the result response policy 404 may include: (1) terminate the call; (2) drop down to the next secure mode and attempt to conduct the call again, (3) drop down from a data call secure mode (data at 64Kbps or 56Kbps) to a voice call secure mode (voice at 56Kbps, 48Kbps, 40Kbps, 32Kbps, or 24Kbps) and attempt to conduct the call again; (4) allow the call to continue in non-secure mode; (5) provide a warning tone or message

indicating to the local call party that the call is not secure; (6) log the event; or (7) send notifications to designated personnel.

[0157] If in step 1338, the TA 102 receives the TA 104-altered alerting or connect message from the PSTN 116, the TA 102 checks the TA 104-altered User-to-User Information IE for the TA 104-inserted codeword in step 1342. The presence of the codeword indicates the TA 104 is VPSTN 100-capable and is ready to conduct the call in secure mode at connect time. If the codeword is not found in the User-to-User Information IE, the called party is considered "not VPSTN 100-capable" (i.e., there is no TA 104 installed in-line at the called party location). In this case, the TA 102 discontinues the secure call setup process 1300 and responds to the failure to setup a secure call in step 1340, pursuant to the TA 102 result response policy 404.

[0158] If the codeword is found in step 1342, the process proceeds to step 1344 wherein the TA 102 checks the User-to-User Information IE for indication of the TA 104 secure mode capabilities. If the TA 104 secure mode capabilities include the bearer capability the TA 102 inserted into the call setup message in step 1314, the TA 102 will proceed to step 1346. If the TA 104 indicates a lower secure mode is necessary, the TA 102 discontinues the secure call setup process 1300 and responds to the failure to setup a secure call in step 1340, pursuant to the TA 102 result response policy 404 (e.g., the result response policy 404 may dictate that the TA 102 teardown the call and drop down to the next secure mode and attempt to conduct the call again).

[0159] In step 1346, the TA 102 modifies the altered alerting or connect message received from the TA 104. The TA 102 restores the original User-to-User Information IE by removing any information inserted by the TA 104 during step 1334, or removes the User-to-User Information IE completely if it contained only information from the TA 104. In step 1348, the TA 102 forwards the restored alerting or connect message to the PBX 114.

[0160] At call connect, the TA 102 and TA 104 know (1) there is a VPSTN 100-capable TA on the other end of the call; (2) the call will be conducted in a secure mode; and (3) the secure mode capabilities (i.e., 64Kbps, 56Kbps, etc.) of each TA; and (4) the secure mode capability to be used. In step 1350, at call connect, the TA 102 and TA 104 send continuous VPSTN DS-0 packets 1180 containing VPSTN DS-0 channel samples with the fixed-bit synchronization pattern in the synchronization/message field 1188 of the packet header 1182 and non-secure media in the payload 1194 (Figure 11D). The TA 102 and TA 104 each detect the synchronization pattern in the exchanged packets and "sync up."

[0161] In step 1352, after the TA 102 and TA 104 sync, the synchronization/message field 1188 is used to exchange additional information, such as compression and encryption options. In step 1354, the synchronization/message field 1188 is used by the TA 102 and the TA 104 to establish and exchange the session's secret key.

[0162] In step 1356, the TA 102 and TA 104 begin encryption of non-secure DS-0 circuit data from their respective PBX, thereby generating the secure VPSTN DS-0 channel sample bit streams (previously discussed with reference to Figures 11A-11C), that each TA

sends to the PSTN 116. The TA 102 and TA 104 decrypt the secure VPSTN DS-0 channel sample bit stream received from the PSTN 116, thereby generating non-secure DS-0 circuit data to send to their respective PBX.

[0163] It is understood that call activity is monitored and analyzed during the life of the call. It is further understood that each security rule base 402 rule is evaluated in sequential order, and the security rule base 402 is exited after any one rule matches the determined call attributes. Although not shown, if the TA 102 or TA 104 detects a change in the call attributes or detects additional call attributes (not available at the time the rule requiring secure mode fired), each rule in their respective security rule base 402, except for the rule already fired by the call's previous attributes, is re-evaluated in sequential order, using the updated attributes. Actions and track functions are then performed based upon the rule matched with the updated call attribute. In the case of a rule firing after another rule has fired, if secure mode is not required by the most recently fired rule, encryption is discontinued and the TA 102 and TA 104 responds to the failure to continue to conduct the call in secure mode in step 1340, pursuant to their respective result response policy 404.

[0164] Referring again to step 1340, it is understood that the result response policy 404 may be configured to dictate select responses based on the determined reason the attempt to conduct the call in secure mode has failed. For example in response to determined reasons such as (1) the TA 102 receives no the altered alerting or connect message in step 1338; (2) the TA 102 finds no codeword in the alerting or connect message in step 1342; and (3) the

TA 104 requests a lower secure mode in the alerting or connect message in step 1344; the result response policy 404 may require the TA 102 to make responses such as: (1) terminate the call; (2) drop down to the next secure mode and attempt to conduct the call again, (3) drop down from a data call secure mode (data at 64Kbps or 56Kbps) to a voice call secure mode (voice at 56Kbps, 48Kbps, 40Kbps, 32Kbps, or 24Kbps) and attempt to conduct the call again; (4) allow the call to continue in non-secure mode.

[0165] If the TA 102 is to drop down to the next secure mode (e.g., from data at 64Kbps to data at 56Kbps), and attempt to conduct the call again, the TA 102 tearsdown the call and returns to step 1314, wherein the TA 102 alters a copy of the original call setup message to now request a data call at 56Kbps (i.e., a bearer capable of supporting digital information at 56Kbps). The TA 102 forwards the new call setup message to the PSTN 116 in step 1316, and steps 1318 through 1344 are repeated.

[0166] If the TA 102 is to drop down from a data call secure mode to a voice call secure mode and attempt to conduct the call again, the TA 102 tearsdown the call and returns to step 1314, wherein the TA 102 inserts a copy of the original call setup message (which requested a voice call). The TA 102 forwards the new call setup message to the PSTN 116 and the call is setup and conducted in secure mode as described with reference to Figures 13C-13E.

[0167] If the TA 102 is to allow the call to continue in non-secure mode, the TA 102 tearsdown the call and returns to step 1314, wherein the TA 102 inserts a copy of the original

call setup message (which requested a voice call). The TA 102 forwards the new call setup message to the PSTN 116 and the call is setup and conducted in the normal, non-secure method used for a call between two phone sets across the PSTN 116.

[0168] Figures 13C and 13D collectively show a process flow diagram for the secure call setup process 1360, whereby secure mode capabilities between the call source TA 102 and the destination TA 104 are autonomously established on a DS-1 circuit which includes T1 access spans (reference will also be made to the elements in Figure 1 for this flowchart).

[0169] In step 1362, an audio connection is established between the telephone 148, PBX 114, PSTN 116, PBX 118, and the telephone 150 in the normal, non-secure method used for connecting two phone sets across the PSTN 116. Once the audio connection is established, two non-secure DS-0 channel data streams flow in a full duplex manner between the two phone sets.

[0170] In step 1364, the TA 102 and TA 104 respectively collect and analyze the call attributes that are available at the time of call connection, as previously mentioned with reference to steps 510-522 of Figures 5A and 5B and steps 912-964 of Figures 9A and 9B. Each TA compares their determined call attributes against their respective security rule base 402. In step 1366, each TA determines if all of their respectively determined call attributes match a security rule base 402 rule (such as the "Secure All Possible Calls" rule previously discussed with reference to Figure 8D), requiring the call to be conducted in secure mode. If the determination is negative, i.e., if no rule is matched in step 1364, or if a rule is matched

that does not require the call to be conducted in secure mode, then the call will be conducted using the normal, non-secure method for conducting a call across the PSTN 116 in step 1368.

[0172] If in step 1364, each TA determines that the fired security rule requires the call to be conducted in secure mode, the TA 102 and TA 104 respond accordingly to perform an autodiscovery, synchronization, negotiation and exchange process to setup a secure call as described below.

[0173] Shortly after audio establishment between the two telephones 148 and 150, an autodiscovery process is executed. In the preferred embodiment of the autodiscovery process, the TA 104, having received an inbound call firing a security rule base 402 rule designating that the call is to be conducted in secure mode, sends a tone to the TA 102 in step 1372. In this process, the tone identifies the TA 104 as being VPSTN-capable.

[0174] In step 1374, the TA 102 receives the tone, and in step 1376, responds by sending "silence" or "comfort noise" to the PBX 114 and a responsive tone to the TA 104. This responsive tone identifies the TA 102 as being VPSTN-capable. The TA 102 then enters a timed delay to allow the TA 104 time to receive the tone and mute its PBX.

[0175] In step 1378, the TA 104 receives the responsive tone from the TA 102, and sends "silence" or "comfort noise" to the PBX 118 in step 1380. If the TA 102 is not VPSTN-capable and does not send a tone in step 1376, the TA 104 times-out while waiting for the response tone in step 1378. If the TA 104 times-out, it discontinues the secure call setup process 1360 and responds to the failure to setup a secure call in step 1382, pursuant to

the result response policy 404. If the TA 104 is not VPSTN-capable and does not send a tone in step 1372, the TA 102 times-out while waiting for the response tone in step 1374. If the TA 104 times-out, it discontinues the secure call setup process 1360 and responds to the failure to setup a secure call in step 1382, pursuant to the result response policy 404.

[0176] In steps 1384 the TA 102 sends to the TA 104, VPSTN DS-0 packets containing VPSTN DS-0 channel samples with the fixed-bit synchronization pattern in the synchronization/message field 1188 of the packet header 1182 (Figure 11D). The TA 102 then enters a timed delay as it waits to receive packets containing the synchronization pattern from the TA 104.

[0177] The TA 104 sends VPSTN DS-0 packets containing the fixed-bit synchronization pattern to the TA 102 in step 1386. If the TA 104 does not receive the synchronization pattern from the TA 102 in step 1387, the TA 104 will generate tones to disable any echo suppressors in the PSTN 116 in step 1388. Echo suppressors, if present, will alter transmitted data.

[0178] In step 1389, if the TA 104 still does not receive the packets containing the synchronization pattern, the TA 104 discontinues the secure call setup process 1360 and responds to the failure to setup a secure call in step 1382, pursuant to the result response policy 404. If the TA 102 times-out while waiting to receive the synchronization pattern from the TA 104 in step 1390, the TA 102 discontinues the secure call setup process 1360

and responds to the failure to setup a secure call, pursuant to the result response policy 404, in step 1382.

[0179] If the TA 102 and TA 104 each receive their respective packets containing the synchronization pattern in either step 1387, 1389, or 1390, they detect the synchronization pattern in the exchanged packets and "sync up" in step 1391.

[0180] Next, the TA 102 and the TA 104 exchange messages to determine the existence of line impairments on the two DS-0 channels flowing between the TA 102 and the TA 104. In steps 1392 and 1395, the TA 102 and the TA 104 send a secured media payload 1194, the content of which is "known" by both TAs. In steps 1393 and 1396, the TA 102 and the TA 104 compare the received payload with the known payload and determine if line impairments changed some of the known bit values during transmission of the respective payloads.

[0181] If in step 1393, the TA 104 determines that bits have changed value during transmission and line impairments are too severe to be overcome by DIL-like processes, the DS-0 channel cannot support the VPSTN process 1200 at the current secure mode level. If this is the case, in step 1394 the TA 104 sends a message telling the TA 102 to discontinue the secure call setup process 1360, and then responds to the failure to setup a secure call in step 1382. Upon receipt of the discontinue message, the TA 102 and management server 106 respond to the failure to conduct the call in secure mode, pursuant to the security policy, in step 1382.

[0182] If in step 1396, the TA 102 determines that bit values have changed during the transmission and line impairments are too severe to be overcome by DIL-like processes, the TA 102 discontinues the secure call setup process 1360. If this is the case, in step 1394 the TA 102 sends a message telling the TA 104 to discontinue the secure call setup process 1360, and then responds to the failure to setup a secure call in step 1382. Upon receipt of the discontinue message, the TA 104 and management server 108 respond to the failure to conduct the call in secure mode, pursuant to the security policy, in step 1382.

[0183] If the TA 102 and the TA 104 determine that bit values have not changed or that line impairments can be overcome by DIL-like processes, the process proceeds to step 1397. The DIL-like processes determine a constellation of symbols representing the control channel 1172 and secure media channel 1174 value to be transmitted. The number of symbols in the constellation indicates the voice call secure mode that can be supported by the side that sent the known value in step 1392 or 1395. The results of the DIL process determines which, if any of the system administrator-allowed secure modes can be used. If none of the administrator-allowed secure modes can be used, the TA 102 and the TA 104 discontinue the secure call setup process 1360 and respond to the failure to conduct the call in secure mode, pursuant to the result response policy 404, in step 1382

[0184] In step 1397, the synchronization/message field 1188 is used to exchange additional information, such as compression and encryption options. In step 1398, the

synchronization/message field 1188 is used by the TA 102 and the TA 104 to establish and exchange the session's secret key.

[0185] In step 1399, the TA 102 and TA 104 begin encryption (or compression and encryption) of non-secure DS-0 circuit data from their respective PBX, thereby generating the secure VPSTN DS-0 channel sample bit streams (previously discussed with reference to Figures 11B-11D), that each TA sends to the PSTN 116. The TA 102 and TA 104 decrypt (or decrypt and decompress) the secure VPSTN DS-0 channel sample bit stream received from the PSTN 116, thereby generating non-secure DS-0 circuit data to send to their respective PBX.

[0186] Referring again to step 1382, it is understood that the result response policy 404 may be configured to dictate select responses based on the determined reason the attempt to conduct the call in secure mode has failed. For example, in response to determined reasons such as (1) the TA 102 receives no tone in step 1374; (2) the TA 104 receives no responsive tone from the TA 102 in step 1378; (3) the TA 104 receives no packets containing the synchronization pattern in step 1387; (4) the TA 104 receives no packets containing the synchronization pattern in step 1389; (5) the TA 102 receives no packets containing the synchronization pattern in step 1390; (6) line impairments between the TA 102 and TA 104 are too severe to overcome in step 1393; and (7) line impairments between the TA 104 and TA 102 are too severe to overcome in step 1396; the result response policy 404 may require the TA 102 to make responses such as: (1) terminate the call; (2) drop down to the next voice

call secure mode (voice at 48 Kbps, 40 Kbps, 32 Kbps, etc.) and attempt to conduct the call again, or (3) allow the call to continue in non-secure mode.

[0187] If the TA 102 or the TA 104 are to allow the call to continue in non-secure mode, coordinating messages are exchanged using the synchronization/message field 1188, encryption and compression are not initiated, and the call is conducted in the normal, non-secure method used for a call between two phone sets across the PSTN 116.

Distributed Deployment

[0188] In Figure 14, reference numeral 1400 designates an alternative embodiment of the VPSTN 100 of Figure 1, featuring a distributed deployment thereof. Due to their distributed nature, many companies are challenged to enforce a telecommunications security policy across their organization. The VPSTN 1400 enables a distributed organization to limit duplication of effort and ensure consistent application of the security policy 302 across multiple locations. Although the VPSTN 1400 components are necessarily distributed, policy can be dictated centrally. This requires an organization to configure and control security devices in a top-down fashion. In order to assess the company-wide security posture, detailed visibility into the entire organizational data stream is provided by collection at the device level, reporting up the management chain, consolidating multiple reports at the management server 106 for viewing, report filtering/configuration, and printing at the client 110.

[0189] The VPSTN 1400 depicted in Figure 14 supports distribution of one or more of the TA 102 (represented by numeral 1402) in remote locations, all interconnected by a TCP/IP-based LAN, private WAN, or the Internet (any of which are identified herein with numeral 1403). With this type of configuration, a geographically separated organization can leverage security expertise in one central location by consolidating the security events and attempt results of the distributed TA 102 with the responses of the management server 106, all on one client 110.

Multi-Tiered Policy-Based Enforcement of a Security Policy

[0190] In Figures 15A and 15B, reference numeral 1500 represents an alternative embodiment of the VPSTN 100 of Figure 1, featuring a system and method of multi-tiered policy-based enforcement of a security policy 1540 across a large, globally distributed enterprise.

[0191] The method of distributed deployment previously discussed and illustrated in Figure 14 is applicable for a small- to medium-sized distributed organization, but processing all the security events from the hundreds of TA 102 that would be deployed in a medium- to large-sized globally distributed enterprise would quickly overload a lone management server 106. Additionally, a single management server 106 would not provide the remote locations with a degree of control over, or visibility into, their own security status.

[0192] As illustrated in Figures 15A and 15B, a management server 106 and client

110 installed at each location (such as San Antonio 1502, San Francisco 1504, Chicago 1506, Washington D.C. 1508, Country *X* 1510, Denver 1512, St. Louis 1514, Pittsburgh 1516, New York City 1518, and Atlanta 1520), will divide traffic load and allow management and implementation of the security policy 1540 on a more localized basis. Unfortunately, deployment of multiple independent VPSTN 100 makes it difficult to ensure the same basic security structure across the enterprise. Additionally, consolidation of local logging information to provide visibility into important local security events at the highest corporate level is difficult and labor-intensive.

[0193] The VPSTN 1500 (i.e., a multi-tiered policy-based enforcement of the security policy 1540 within a distributed architecture), ensures implementation of a basic, enterprise-wide security policy 1540 with a degree of localized policy control, as well as automatic security event log consolidation and visibility into important local security events at the highest corporate level.

[0194] As shown in Figures 15A and 15B, within a multi-tiered management environment, a "corporate" level 1522 management server 1528 oversees its own local management server 106 at San Antonio 1502 as well as multiple "regional" level 1524 management servers 106 at San Francisco 1504, Chicago 1506, and Washington D.C. 1508. These "regional" management servers oversee multiple "branch" level 1526 management servers 106 at Country *X* 1510, Denver 1512, St. Louis 1514, Pittsburgh 1516, New York City 1518, and Atlanta 1520. Each management server 106 within the multi-tiered

environment 1500 enforces the security policy 1540 for its local one or more TA 102, and in accordance with the management server tier position, may also oversee management servers below it. Each location is interconnected by a TCP/IP-based LAN, private WAN, or the Internet (any of which are identified herein with numeral 1530). For the purpose of simplification, the examples will pertain to the "corporate" level 1522 management server 1528 in San Antonio 1502 overseeing the "regional" level 1524 management server 106 in San Francisco 1504, which will oversee the "branch" level 1526 management server 106 in Country *X* 1510 and the "branch" level 1526 management server 106 in Denver 1512.

[0195] Just as a CEO imparts guidelines of conduct to his VPs, who in turn impart fundamentally similar guidelines to their Directors, so does the "corporate" level 1522 management server 1528 define a basic security policy 1540 to the "regional" level 1524 management server 106 in San Francisco 1504, that in turn disseminates a fundamentally similar security policy to the "branch" level 1526 management server 106 at Country *X* 1510 and Denver 1512.

[0196] For example, a corporate-dictated security policy 1540 will contain basic rules (i.e., a security rule base 1542 and a result response policy 1544). These rules are classified as either "Required" or "Optional". Each level of the hierarchical environment must adhere to a required rule, but can choose to ignore optional rules. Each level of the tier is capable of making their local rules and the rules for the tiers below it more stringent than the corporate-dictated rules, but can not make the rules more lax. In this way, a basic

security structure is ensured across the enterprise.

[0197] The corporate-dictated security policy 1540 contains basic security rules that dictate what information will be reported upward, thereby providing visibility into only the most important local security events at the corporate level. Just as the corporate-dictated rules send security guidelines that may become more stringent as the rules are passed downward, the policy institutes an information filter that becomes more selective as electronic mail, logs and reports, etc., are routed upward. The tasks in the "Tracks" column of the corporate-dictated rule (such as electronic mail notification, pager notification, logging of events, etc.), that are of interest at a local level but are not of interest at higher levels, are designated to be filtered out if notification of a rule firing is to be routed up the tier. All logging is real-time, both at the location where the event occurs and at upper levels of the organization that, pursuant to the security policy 1540, may or may not require notification of the event.

[0198] Figures 15C, 15D and 15E, collectively illustrate rules in an exemplary security rule base 1542, for use in implementing multi-tiered policy-based enforcement of the security policy 1540. Although not shown, it is understood that the result response policy 1544 is similarly configured. As previously mentioned with respect to the security rule base 402 shown in Figure 4 and Figures 7A-7B, rules based upon call attributes including "Direction;" "Source;" "Destination;" "Call type;" "Date;" "Time;" and "Duration"(not shown); implement an "Action" (allow or deny the call); other additional actions and

logging, reporting and notification functions, "Track." Additionally, each rule has the TA 102 deployment location/identifier "Install On", allowing an enterprise to implement one single security rule base 1542 containing rules designated to be applied in specific locations. As shown in Figures 15C-15E, when implementing multi-tier policy-based enforcement, the attributes of the rules are expanded to include "Class", a classification of adherence to a rule as either "Required" or "Optional" or "Local". Any rule that is not a corporate-dictated rule will be designated as a local rule. If notification of a rule "firing" is to be routed up the tier to the management server 1528, "Route" will appear in the "Track" column, dictating that when a management server 106 is notified by a subordinate management server 106 that a rule has fired, the notification will be routed upward to the next higher-tiered management server 106. Additionally, if notification of a rule "firing" is to be routed upward, tasks listed in the "Track" column are designated to be filtered (F), if execution of the task should take place only at the location where the rule originally fired and the local TA 102 notified the management server 106. By filtering the tasks in the "Track" column, the policy will designate which tasks, such as event logging will be performed at each level of the tier, when a rule "fires" at a subordinate level of the tier.

[0199] Rules 1-10, are explained as follows, it being understood that the security rule base 1542 for multi-tiered policy-based enforcement of the security policy 1540 shown in Figures 15C-15E may include any number and types of rules, and that each rule is evaluated in sequential order, exiting after any one rule matches all the call criteria.

Rule 1:

[0200] This rule states "Deny outbound calls from extensions in the VPSTN non-secure group, generate an electronic mail and page, and log the call." This rule is installed on all TA 102. This rule identifies and segregates lines and denies calls over the lines which are in the VPSTN non-secure group and logs the call for accounting purposes. Adherence to this rule is required. Since the firing of this rule is an indication of security posture, it is of interest to the upper echelon. As notification of the rule "firing" is made at each upper level of the hierarchy, the event is logged, but electronic mail and pager notification is filtered out. Note that (F) designates that the tasks of generating electronic mail and pager notification is filtered out. Generation of an electronic mail and pager notification takes place only at the location where the TA 102 notifies the management server 106 that the rule "fired."

Rule 2:

[0201] This rule states "Deny inbound calls to extensions in the VPSTN non-secure group, generate an electronic mail and page, and log the call." This rule is installed on all TA 102. This rule identifies and segregates lines and denies calls over the lines which are in the VPSTN non-secure group and logs the call for accounting purposes. Adherence to this rule is required. Since the firing of this rule is an indication of security posture, it is of interest to the upper echelon. As notification of the rule "firing" is made at each upper level of the hierarchy, the event is logged, but electronic mail and pager notification is filtered out. Generation of an electronic mail and pager notification takes place only at the location where

the TA 102 notifies the management server 106 that the rule "fired."

Rule 3:

[0202] This rule states "Allow inbound fax calls to extensions in the fax group between 9pm and 6am, conduct the call in secure mode, and log the call." This rule is installed on all TA 102 in San Antonio 1502. This rule causes all inbound fax calls to a specified inbound destination during a specified time to be conducted in secure mode and logs the call for accounting purposes. This rule is local to San Antonio 1502 and the upper level of the tier is not notified that the rule "fired."

Rule 4:

[0203] This rule states "Allow inbound modem calls to extensions in the daily receivable modem group, conduct the call in secure mode, and log the call." This rule is installed on all TA 102 in San Antonio 1502. This rule causes all inbound modem calls to a specified inbound destination to be conducted in secure mode and logs the call for accounting purposes. This rule is local to San Antonio 1502 and the upper level of the tier is not notified that the rule "fired."

Rule 5:

[0204] This rule states "Allow all outbound international voice, fax, modem, and VTC calls to Country *X*, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all outbound voice, fax, modem, and VTC calls to any destination within Country *X* to be conducted in secure mode and logs the call for

accounting purposes. Adherence to this rule is required. Upper levels of the tier are not notified that the rule "fired."

Rule 6:

[0205] This rule states "Allow all inbound international voice, fax, modem, and VTC calls from Country *X*, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all inbound voice, fax, modem, and VTC calls from any source within Country *X* to be conducted in secure mode and logs the call for accounting purposes. Adherence to this rule is required. Upper levels of the tier are not notified that the rule "fired."

Rule 7:

[0206] This rule states "Allow inbound and outbound voice, fax, modem, and VTC calls between extensions in the inter-branch groups, conduct the call in secure mode, and log the call." This rule is installed on all TA102. This rule causes all inbound and outbound voice, fax, modem, and VTC calls to and from specified sources and destinations to be conducted in secure mode and logs the call for accounting purposes. Adherence to this rule is required. Upper levels of the tier are not notified that the rule "fired."

Rule 8:

[0207] This rule states "Allow outbound voice, fax, modem, and VTC calls from extensions in the exec staff and engineering groups, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all outbound voice, fax,

modem, and VTC calls from specified outbound sources to be conducted in secure mode and logs the call for accounting purposes. Adherence to this rule is optional but recommended for security purposes. Upper levels of the tier are not notified that the rule "fired."

Rule 9:

[0208] This rule states "Allow inbound voice, fax, modem, and VTC calls to extensions in the exec staff and engineering groups, conduct the call in secure mode, and log the call." This rule is installed on all TA 102. This rule causes all inbound voice, fax, modem, and VTC calls to specified inbound destinations to be conducted in secure mode and logs the call for accounting purposes. Adherence to this rule is optional but recommended for security purposes. Upper levels of the tier are not notified that the rule "fired."

Rule 10:

[0209] This catch-all rule states "Deny all calls, generate an electronic mail and log the call." This rule is installed on all TA 102. Adherence to this rule is required. At first glance, this rule seems to deny any call to or from anywhere. This is not the case. This rule is typically placed at the bottom of the sequential list of rules to deny and log all calls that do not fit into any of the preceding rules. Since this rule is typically placed at the bottom of the sequential list of rules to deny and log all calls that do not fit into any of the preceding rules, the firing of the rule is an indication of the security posture, and of interest to the upper echelon. As notification of the rule "firing" is made at each upper level of the hierarchy, the event is logged, but the electronic mail notification is filtered out. Generation of an

electronic mail notification takes place only at the location where the TA 102 notifies the management server 106 that the rule "fired." Again, each rule is evaluated in sequential order, exiting immediately after any one rule matches all the call criteria.

[0210] Figure 15F is a process flow diagram 1550 illustrating the implementation of a multi-tiered policy-enforcement of the security policy 1540. It is understood that this process can be implemented during step 506 and 508 of the installation, configuration, and operation process discussed previously in Figures 5A and 5B, or at any time afterward, since the corporate-dictated rules will have priority over and remove any conflicting local rule.

[0211] Referring to Figure 15F, in step 1552, corporate-dictated rules, similar to those described previously with reference to Figures 15C-15E, are defined. The corporate-dictated rules are included in the basic security policy 1540 that is distributed downward from the "corporate" level 1522 management server 1528 to each "regional" level 1524 management server 106 (such as the one in San Francisco 1504), and to each "branch" level 1526 management server 106 (such as those in Country *X* 1510 and Denver 1512). In step 1554, the corporate-dictated rules are merged into the current security policy 1540. As mentioned previously, the corporate-dictated rules will have priority over and remove any conflicting rules. In step 1556, the updated security policy 1540 is downloaded to the local TA 102 on the "corporate" level 1522.

[0212] Steps 1558-1564 illustrate a recursive process by which the updated security policy 1540 is downloaded to each management server 106 and its associated TA 102 on

each level 1524 and 1526 of the tier, until the process has been performed on the lowest level of the tier. In particular, in step 1558, the updated security policy 1540 is sent to the management servers 106 on the "regional" level 1524; e.g. the management server 106 in San Francisco 1504. In step 1560, the new corporate-dictated rules are merged with the currently existing rules in the San Francisco 1504 management server 106.

[0213] In step 1562, the updated security policy 1540 is downloaded to the local TA 102 of the San Francisco 1504 management server 106. In step 1564, a determination is made whether the current level (in this case, the San Francisco 1504 management server 106), is the last level of the tier or whether it has supervisory responsibilities of other management servers, such as those on the "branch" level 1526. If it is determined that the current level is not the last level of the tier (i.e., the current management server 106 has supervisory responsibilities), execution returns to step 1558 and steps 1558-1562 will be repeated; as will be the case for the dissemination of the new security policy 1540 to the management server 106 in Country *X* 1510 and Denver 1512. If a positive determination is made in step 1564, i.e., when the corporate-dictated rules have been disseminated to the management servers 106 and the TA 102 populating each level of the tier, the process is complete and execution terminates in step 1566.

[0214] It should be understood that the rules comprising this basic security structure can be modified and sent down the tier at any time. While the corporate-dictated rules can be modified completely at the "corporate" level 1522 and pushed downward, the security

administrators on other levels, such as the "regional" level 1524, can only accept the rules as is or make the rules to be sent downward to the "branch" level 1526 more stringent.

[0215] Figure 15G is a process flow diagram 1580 illustrating the implementation of filtering on logging and execution of other "Track" tasks in a multi-tiered policy-enforced environment. It is understood that this filtering process can be applied to any task that may occur in the "Track" column of the security policy 1540.

[0216] Referring to Figure 15G, in step 1582, the TA 102 evaluates the attributes of a call (direction, source, destination, type of call, etc.), against the sequential list of rules in the security policy 1540. When an applicable rule is found, the rule "fires" and the TA 102 enforces the rule. In step 1584, the TA 102 notifies its associated management server 106 that the specific rule has fired and that the rule has been enforced. In step 1586, the management server 106, pursuant to the rule in the security policy 1540, automatically executes the tasks designated in the "Track" column of the rule, such as generating an electronic mail notification and logging the event.

[0217] Steps 1588-1592 illustrate a recursive process by which the management server 106 on each level of the multi-tiered hierarchy receives notification of the rule having been fired, executes "Track" tasks for the rule, and notifies its supervisory management server 106 that the rule has "fired," until the notification reaches the top level of the tier. In particular, in step 1588, the rule is evaluated to determine if it is a corporate-dictated rule, and if notification of the rule "firing" will be routed up the tier in accordance with the

"Route" task in the "Track" column. If the notification of the rule firing is to be routed upward, execution proceeds to step 1590, in which the management server 106 will send a notification of the rule firing to its supervisory management server 106.

[0218] Execution then proceeds to step 1592, in which, upon receiving notification routed from a subordinate management server 106 that a rule has fired, the supervisory management server 106 will execute all "Track" tasks in the rule, such as logging, that are not filtered, and then route a notification of the rule firing to its supervisory management server 106. Execution then returns to step 1588. This recursive process will continue until the notification and logging reach the "corporate" level 1522 management server 1502 which will consolidate all logging and reports for the enterprise. Referring again to step 1588, if a negative determination is made, execution terminates in step 1594.

Virtual Private Switched Telecommunications Network Complemented with Computer Telephony Integration Interface

[0219] It is understood that the VPSTN 100 can take many forms and embodiments. For example, the VPSTN 100 may be complemented with computer telephony integration (CTI) interface(s) to specific PBXs 114. In this alternate embodiment, the VPSTN 100 may issue commands to the PBX 114 (via the CTI interface), for the PBX 114 to perform designated actions on the call. Additionally, the PBX 114 may provide designated call attributes to the VPSTN 100 (via the CTI interface), for use in applying the security rule-set to the call. Action commands issued to, and call attributes provided by the PBX 114 are

pursuant to the rule-set and within PBX 114 capabilities.

[0220] In Figure 16, the reference numeral 1600 represents an alternate embodiment of the VPSTN 100 shown and described in Figure 1 and Figure 2, whereby the VPSTN 100 is complemented with a CTI interface 1602 to PBX 114. Accordingly, all previously described operations and functions of the VPSTN 100 are hereby inserted by reference into the VPSTN 1600.

[0221] The VPSTN 1600 consists primarily of the TA 102 connected in-line between the end-user stations 136 of an enterprise and the stations' connections into the PSTN 116 at the TA 206. Ethernet cabling and a serial port connection (or special connection) 1604 connects the TA 206 to the CTI interface 1602, which is connected to or located within the PBX 114.

[0222] In this embodiment, the PBX 114 provides call attribute information to the TA 206 via the CTI interface 1602, for the process of detecting and analyzing call activity discussed previously with reference to step 510 in Figure 5A, and Figures 9A and 9B. Call attributes provided by the PBX 114 to the TA 206 are limited only by user configuration and the PBX 114 capabilities, and may include, for example: station extension, trunk, channel, inbound call number, outbound call number, call type, call date, call time, call duration. It is understood that the call attributes described herein as provided by the PBX 114 are expanded upon pursuant to PBX 114 capabilities. Different combinations of TA 206-provided and

PBX 114-provided attributes are contemplated, such that all or only selected attributes are provided by the PBX 114.

[0223] Additionally, in this embodiment, the TA 206 issues commands to the PBX 114 via the CTI interface 1602, and thereby tasks the PBX 114 to perform actions and track functions associated with the call, pursuant to the security policy 302, during the process of security policy enforcement discussed previously with reference to steps 512-528 in Figures 5A-5B, and Figures 10A and 10B. Action and track function commands sent to the PBX 114 are limited only by user configuration and the PBX 114 capabilities, and may include, for example: allow the call, deny (terminate) the call, conduct the call in secure mode, generate electronic mail, pager, console messaging, and SNMP notifications, and log the event. It is understood that the actions and track functions described herein as performed by the PBX 114 are expanded upon pursuant to PBX 114 capabilities. Different combinations of TA 206-performed and management server 106-performed actions and PBX 114-performed actions are contemplated, such that all or only selected actions and track functions are performed by the PBX 114.

[0224] It is understood that the present invention can take many forms and embodiments. The embodiments shown or discussed herein are intended to illustrate rather than to limit the invention, it being appreciated that variations may be made without departing from the spirit of the scope of the invention. For example, any number of different rule criteria for the security policy may be defined. Different attributes and rules are

contemplated. The algorithms and process functions performed by the system may be organized into any number of different modules or computer programs for operation on one or more processors or workstations within the system. Different configurations of computers and processors for the system are contemplated, including those in which the functions of the management server 106 may be inserted into the system at the TA 102. The programs used to implement the methods and processes of the system may be implemented in any appropriate programming language and run in cooperation with any hardware device. The system may be used for enterprises as small as a private home or business with just a few lines as well as for large enterprises with multiple PBX locations around the world, interconnected in one or more private networks or virtual private networks. In the case where multiple extensions are involved, it is understood that the extensions may be PBX extensions or direct line extensions.

[0225] Although illustrative embodiments of the invention have been shown and described, it is understood that a wide range of modifications, changes and substitutions are intended in the foregoing disclosure, including various encryption engines, encryption algorithms, compression algorithms, resulting word block sizes, key exchange schemes, DS-0 channel sample configuration and content, and methods of autodiscovery. In some instances, some features of the invention will be employed without a corresponding use of other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.